ALSO Training – Fortinet Security Fabric

13./14.06.2017, Zurich, Renens, Emmen

Gabriel Kälin, Channel Systems Engineer

gkaelin@fortinet.com, +41 79 882 80 98

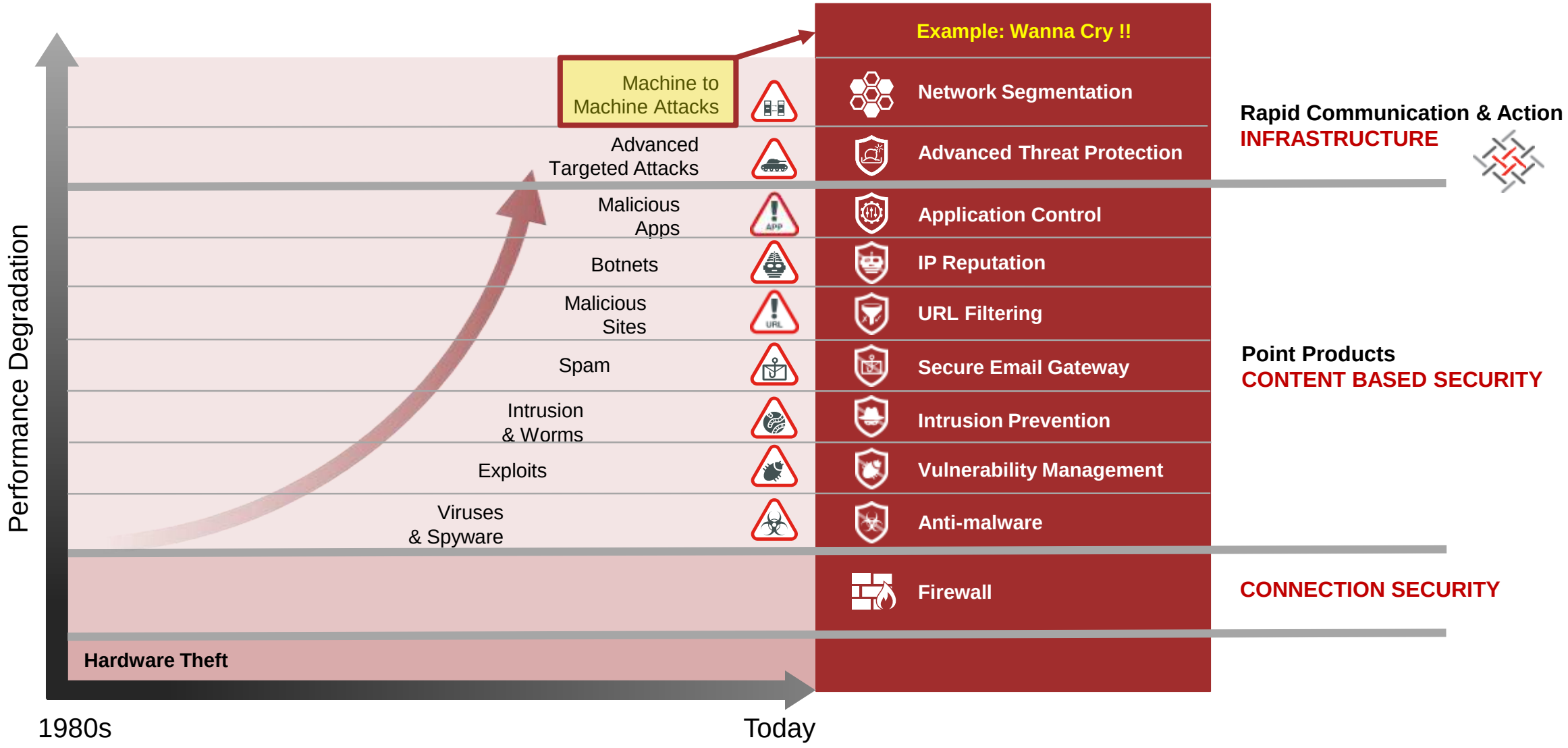
What You Can Learn in this Training

- Security Fabric Vision
  - Tight mesh of interconnected security controls
- Broad solution
  - Be informed about your environment, regardless what it looks like
  - Demo FortiView
- Powerful solution
  - Don’t let security be an inhibitor, but an enabler
  - Security Fabric Audit demo
- Automated solution – profit to the max
  - Coordinated Advanced Threat Protection – demo
  - Go beyond FortiWorld

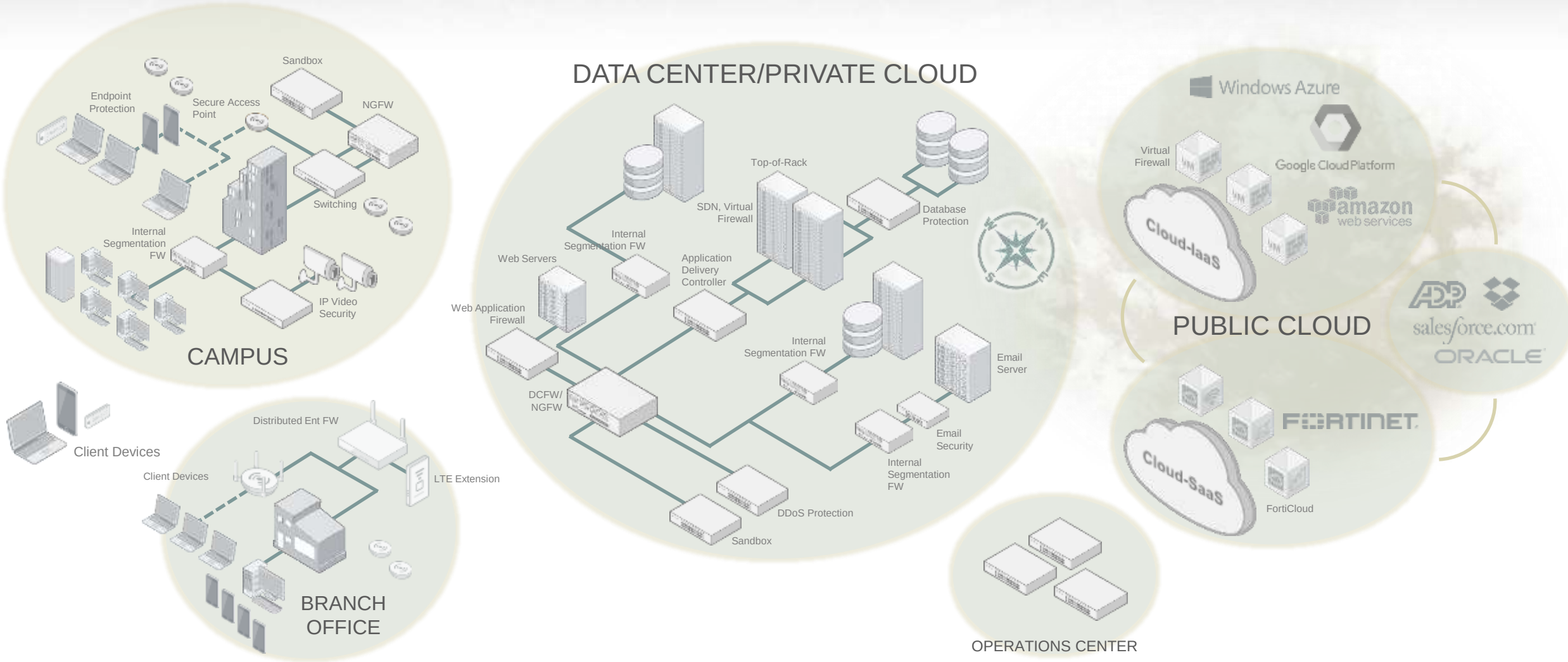
The Vision: Fortinet Security Fabric

Address today’s threats with a tight mesh of interconnected security controls

The Threat and Performance Challenge Timeline

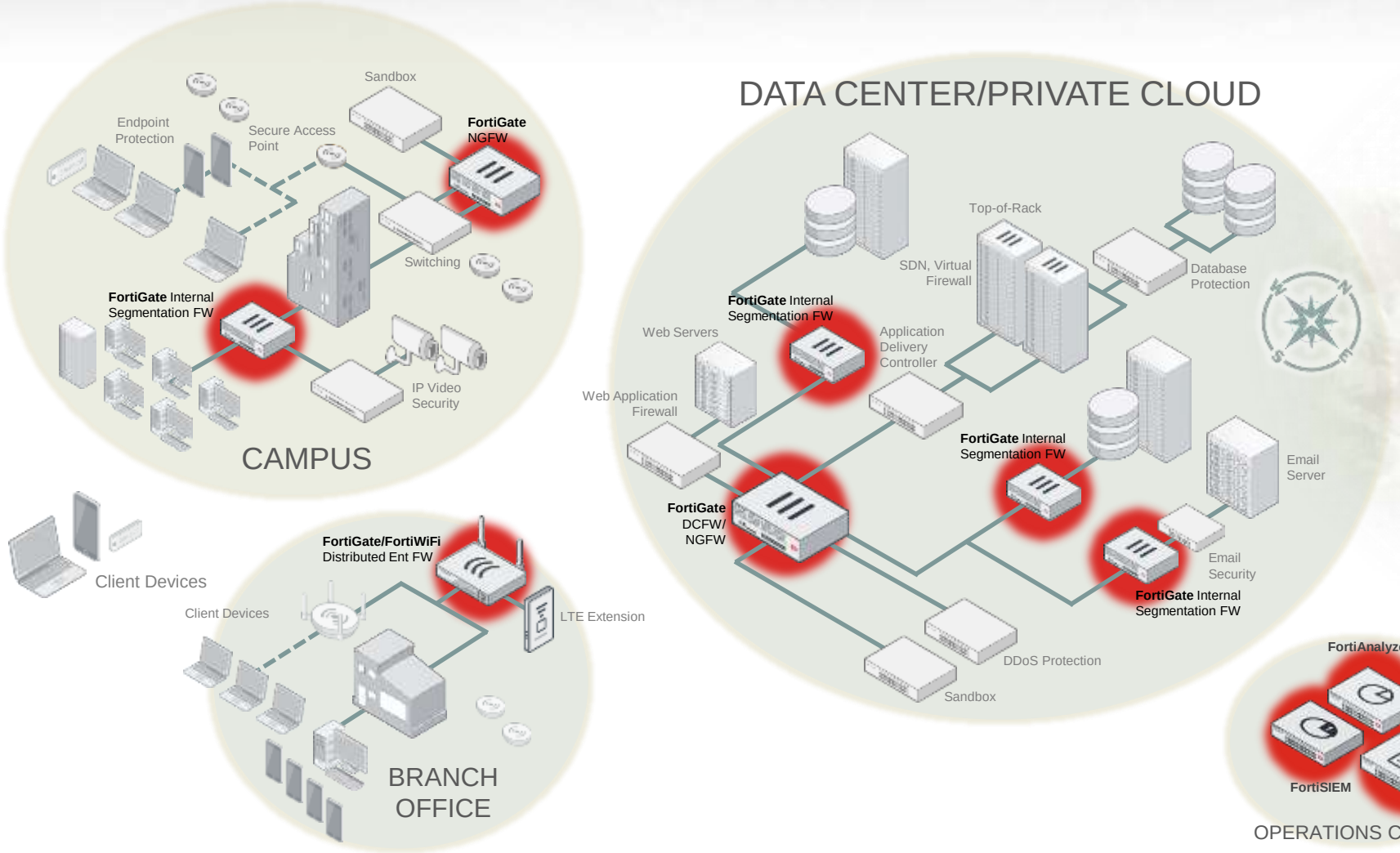


A Typical Enterprise Deployment Today



It All Starts with Fortinet Enterprise Firewalls

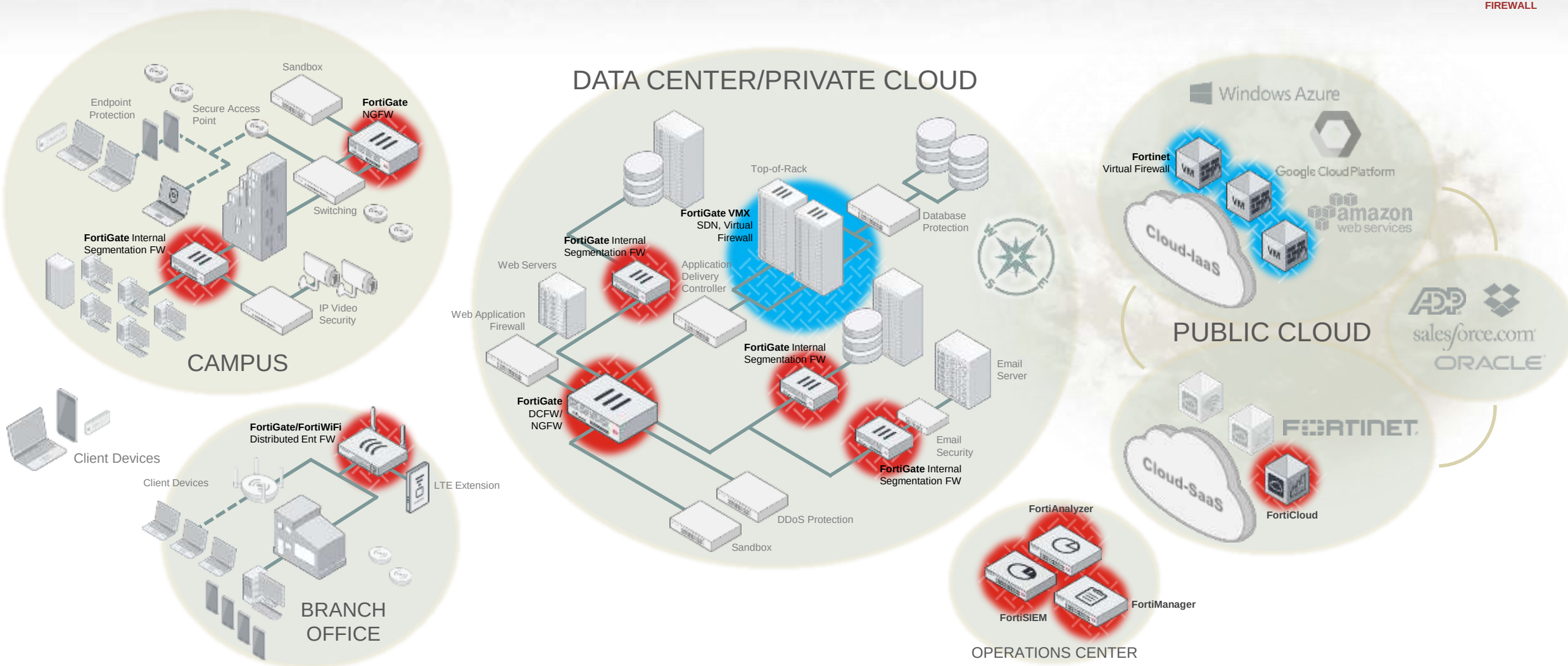
ENTERPRISE FIREWALL



Regardless of Location or Form Factor

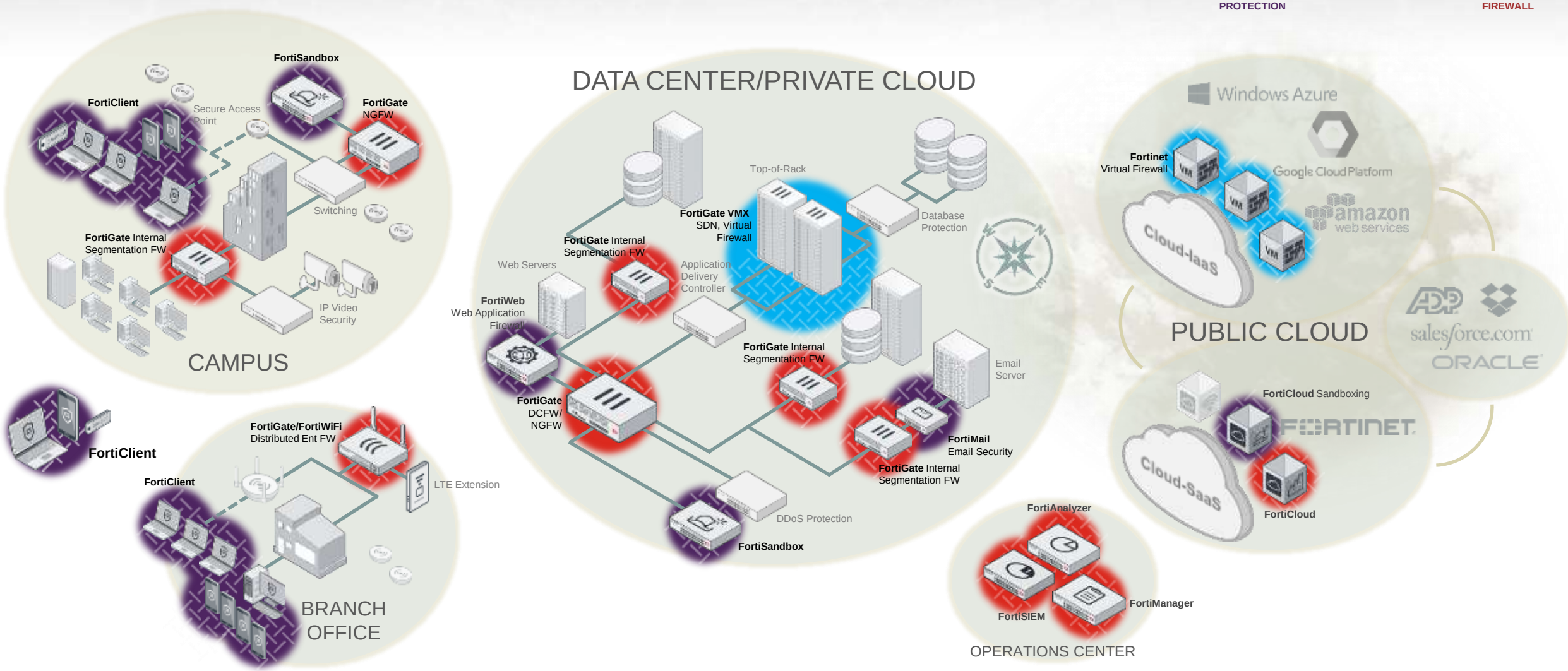
CLOUD SECURITY

ENTERPRISE FIREWALL



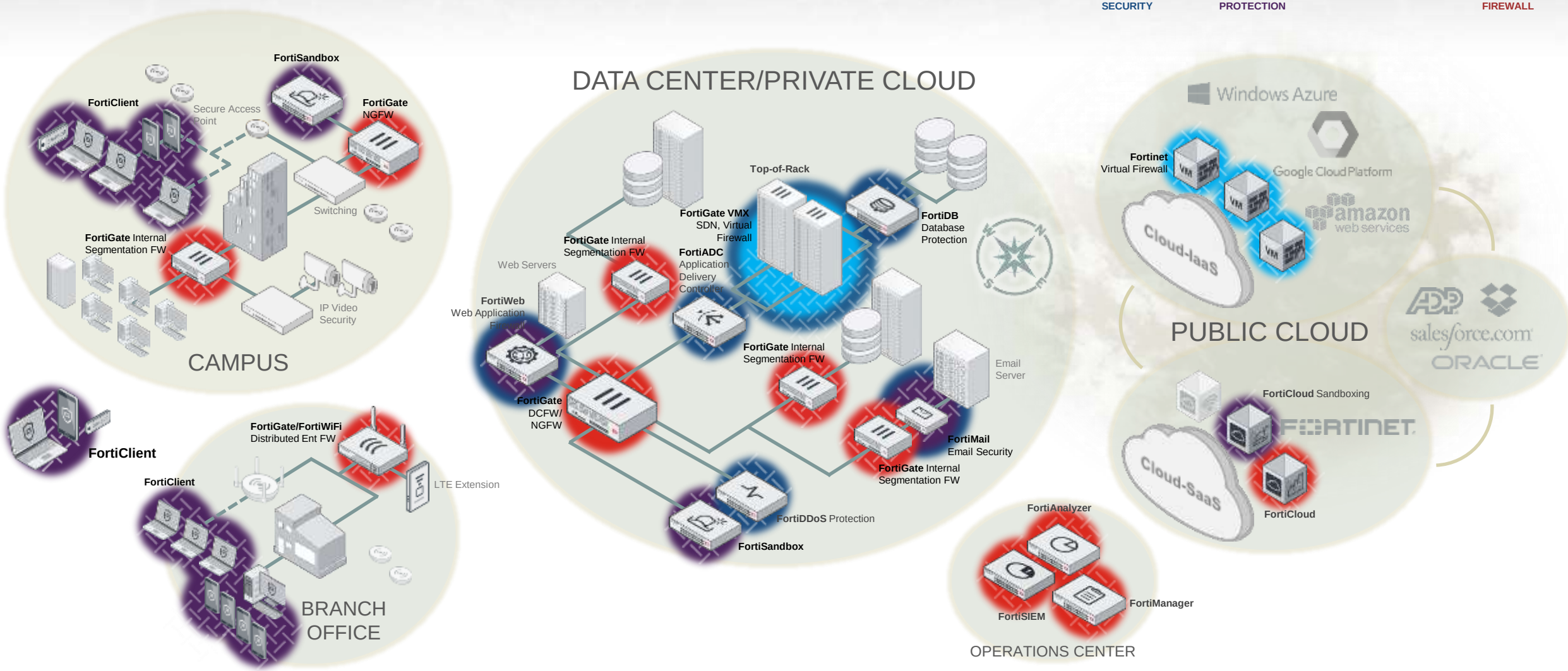
Local Threat Intelligence with the ATP Solution

ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL



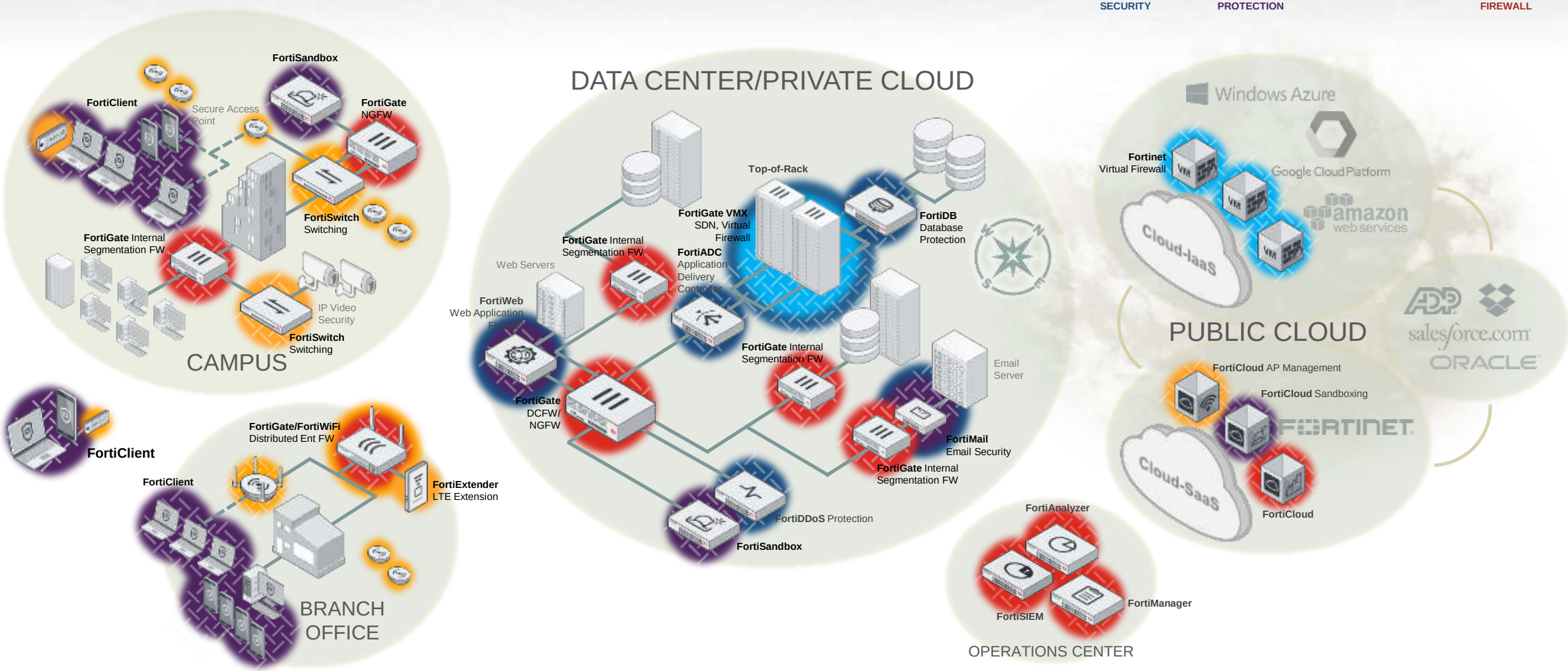
Including the Application Layer

APPLICATION SECURITY | ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL

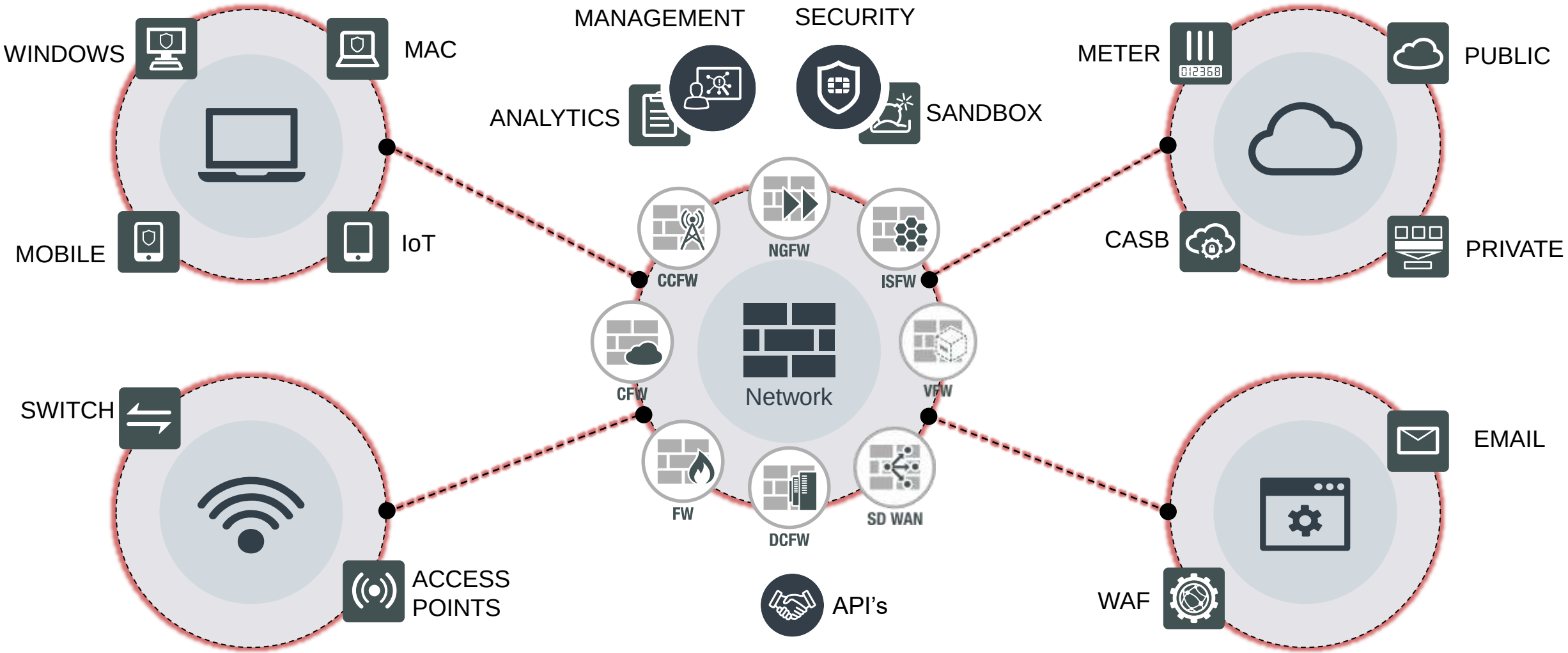


… and the Endpoint and Access Infrastructure

SECURE ACCESS | APPLICATION SECURITY | ADVANCED THREAT PROTECTION | CLOUD SECURITY | ENTERPRISE FIREWALL



Span of the Security Fabric



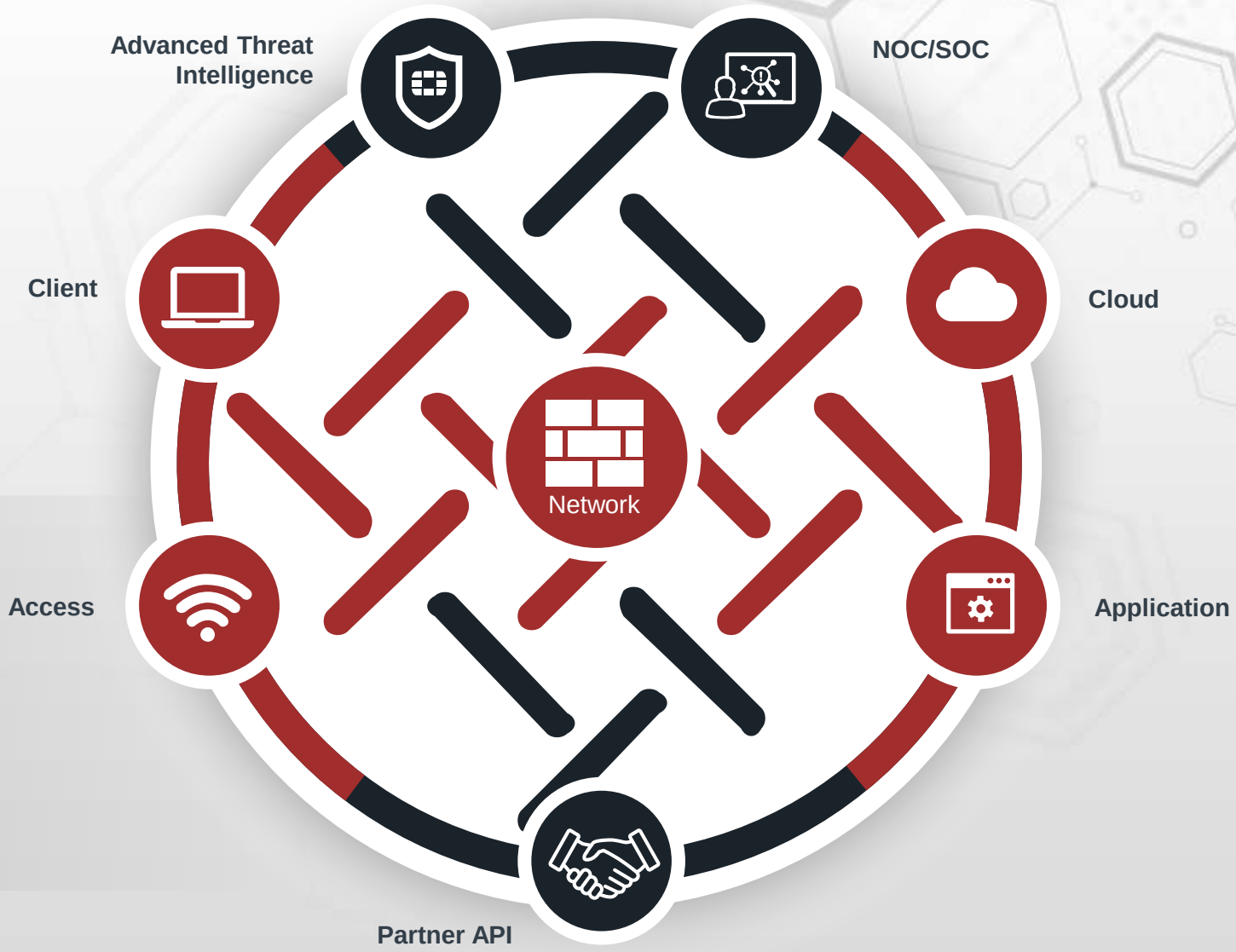
FORTINET SECURITY FABRIC

The Fortinet Security Fabric is the vision that delivers on the promise of Security without Compromise:

BROAD

POWERFUL

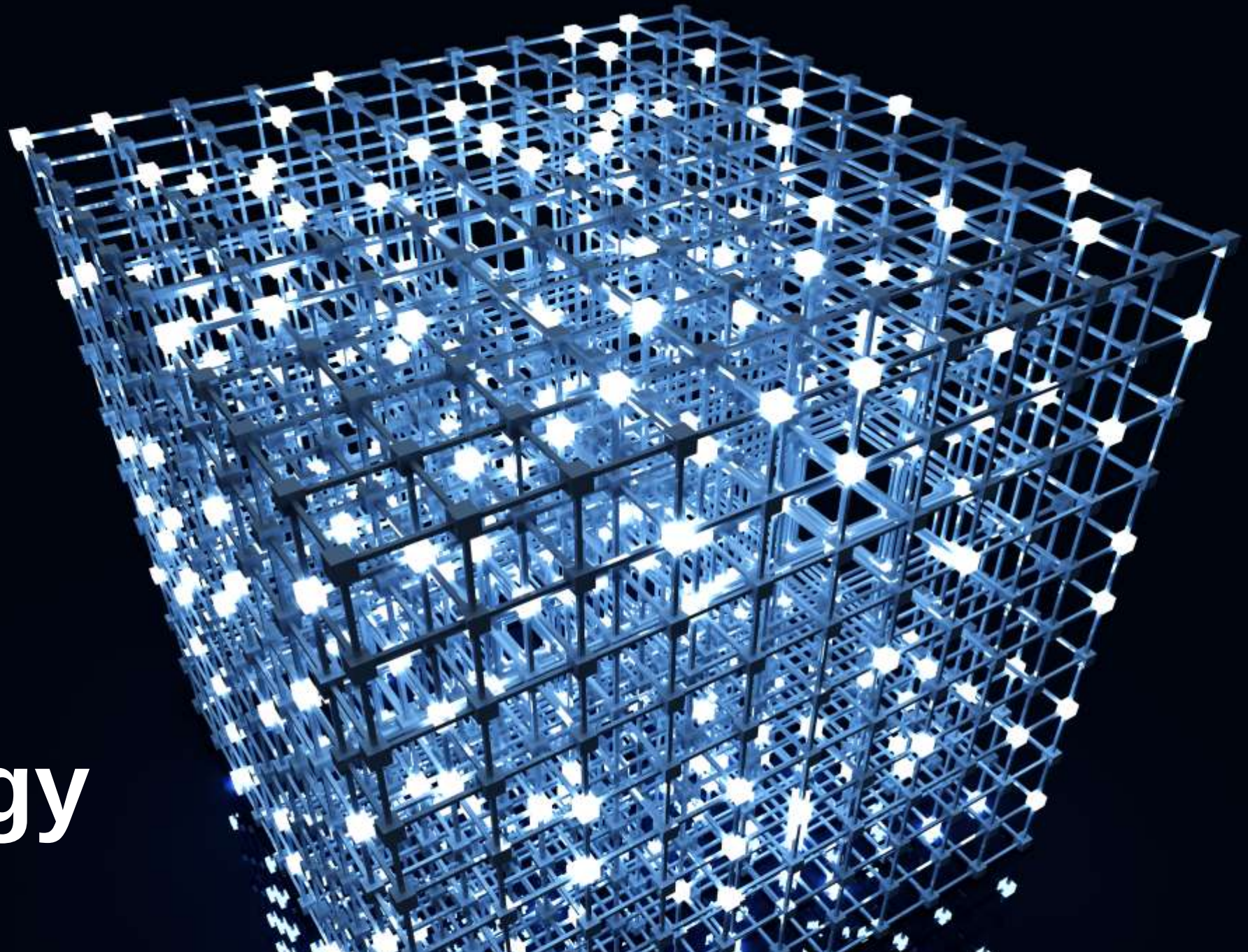
AUTOMATED



BROAD

Deeper **visibility and control** throughout the Security Fabric
to reduce the attack surface from IoT to Cloud

Fabric Topology Views



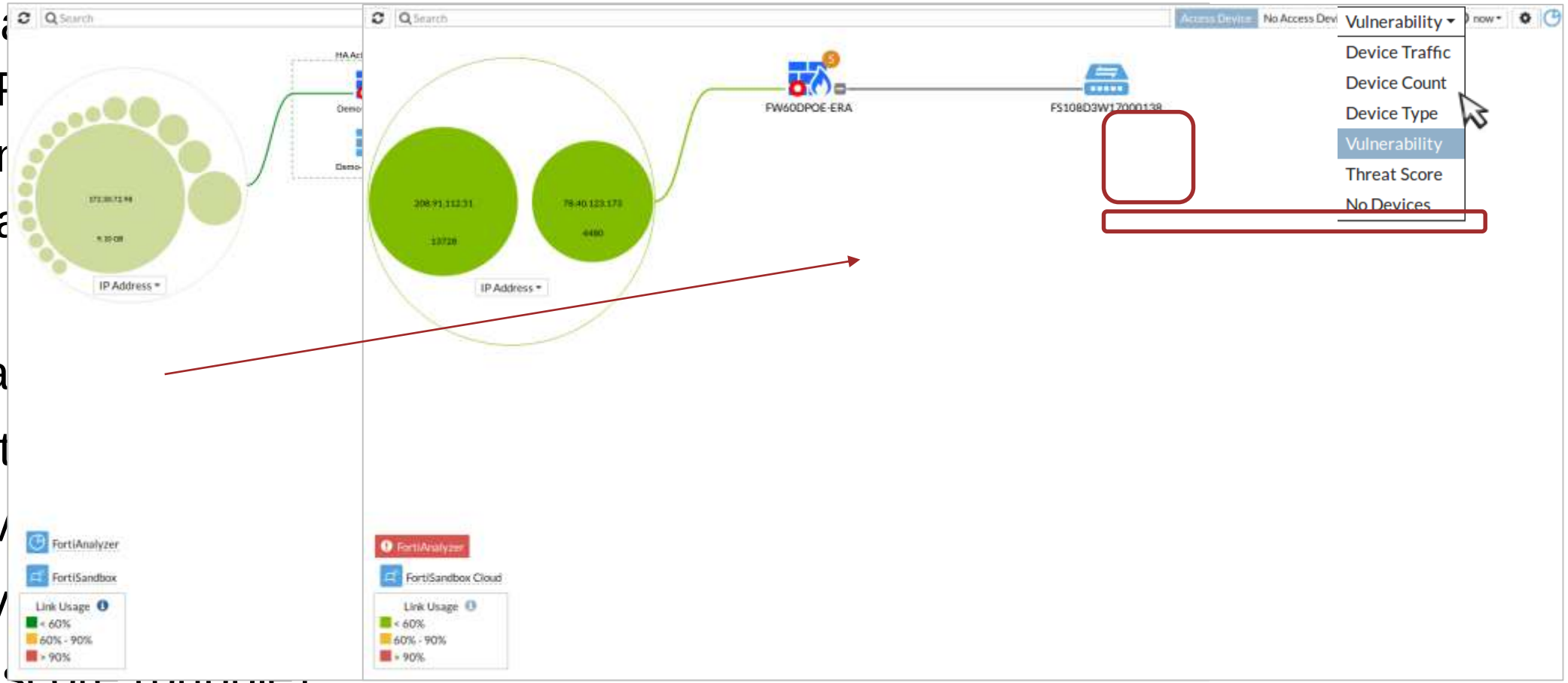
Network Topologies

- Segmentation brings more complexity to network topologies.
  - » It becomes easy to make mistakes we can hardly see afterwards
  - » Congestions and bottlenecks get harder to locate

Fabric Topology View

- Fabric Topology Views are now added to 5.6
  - » FortiG
  - » FortiA
  - » FortiAr
  - » FortiSa
- Endpoint
- Links usa
- User avat
- OS & dev
- Rank dev

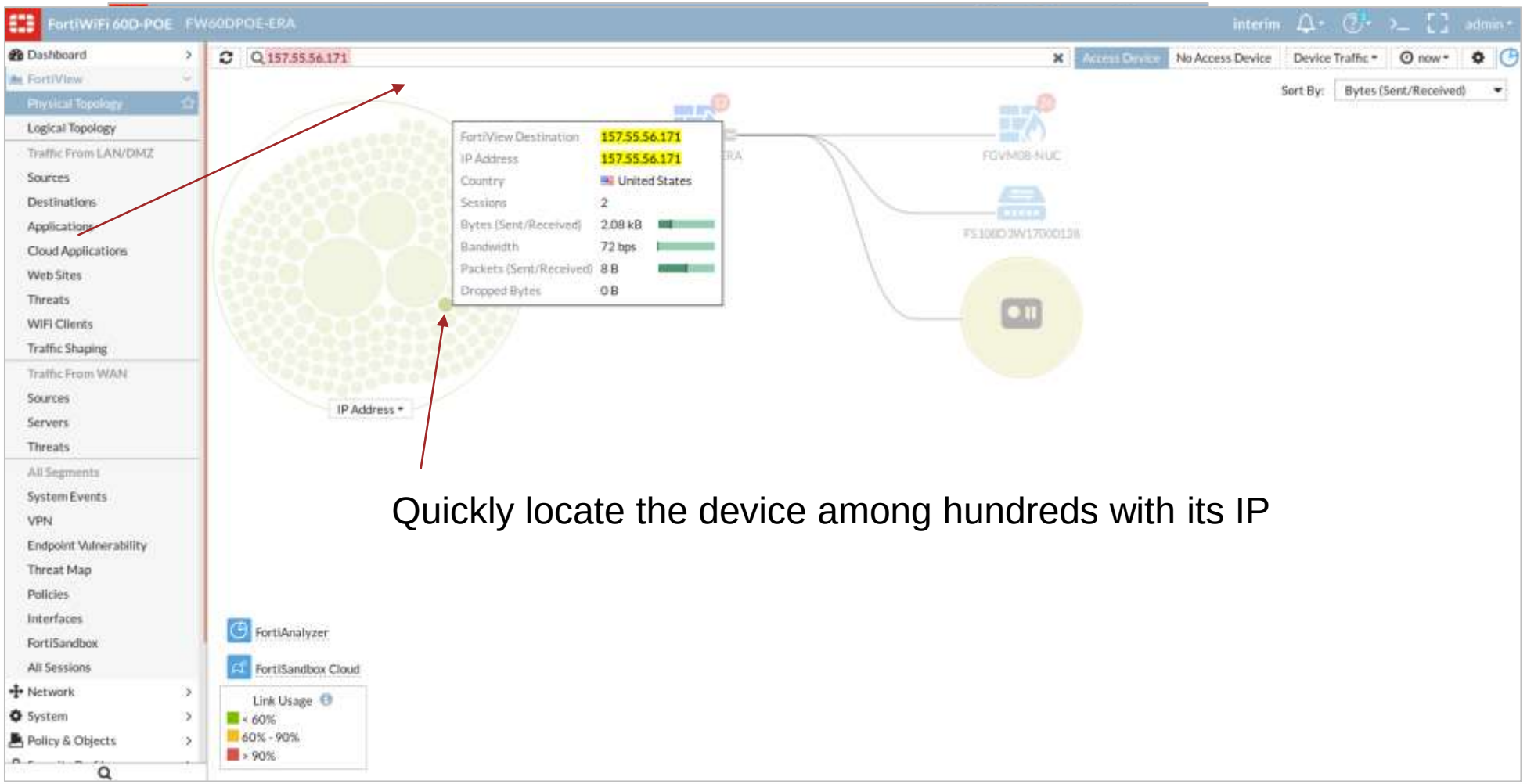
FortiClient score (bubble)



“Search” feature in topology

- Helps to quickly locate and size relevant information

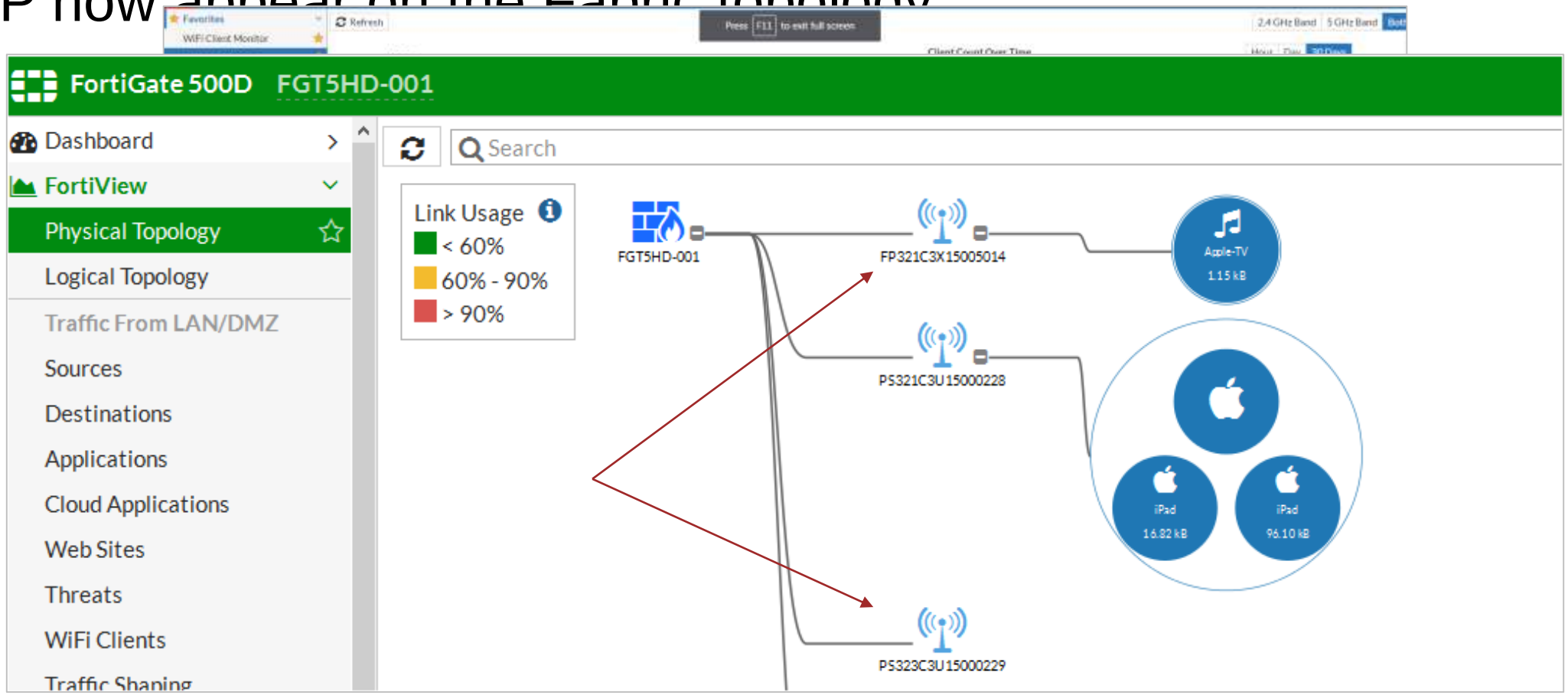
Search for A specific information (device…)



Quickly locate the device among hundreds with its IP

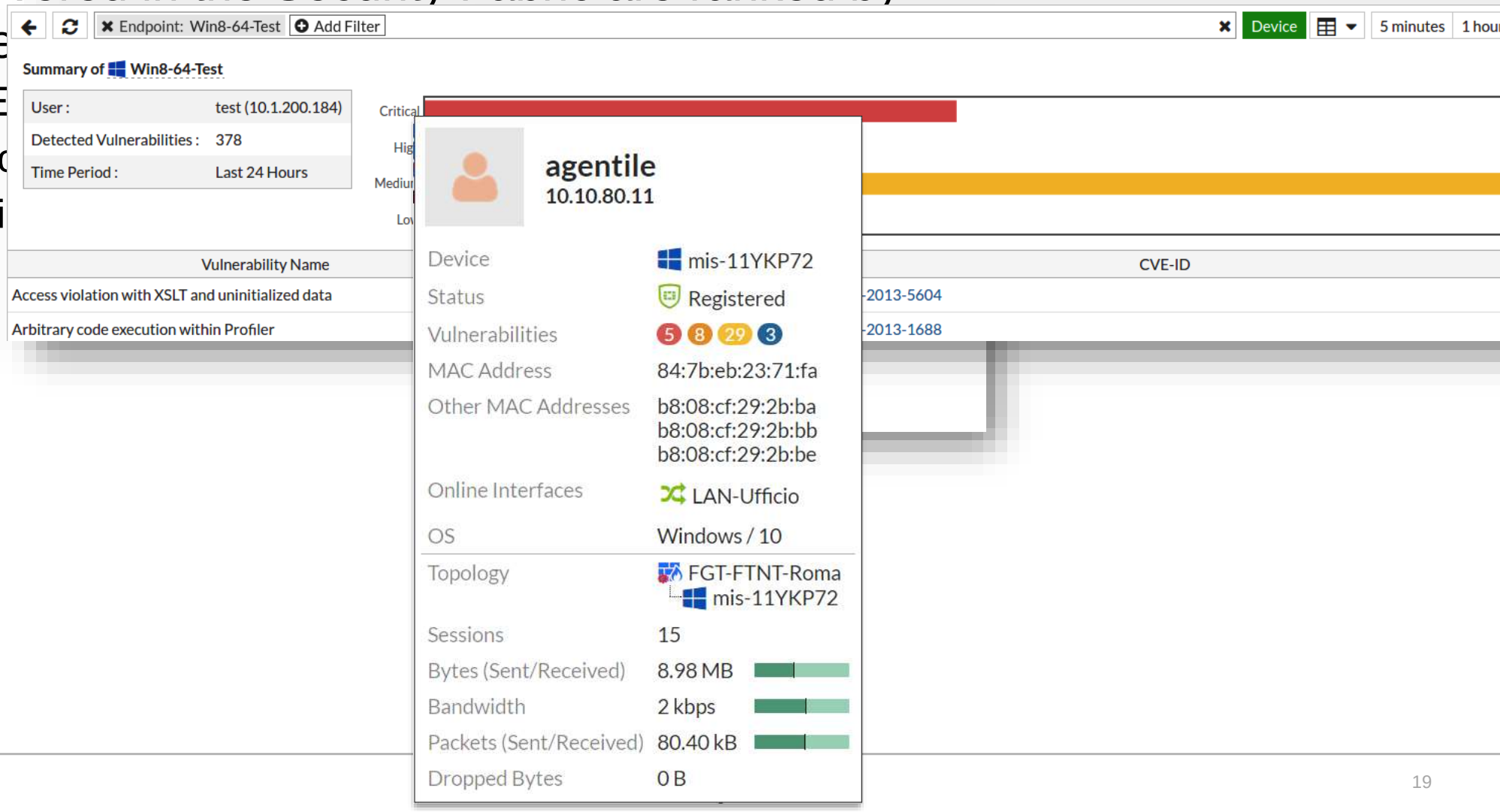
Better visibility on wireless network

- New fortiview Wifi Health Monitoring
- AP now appear on the Fabric topology



Visibility on Endpoints Vulnerability

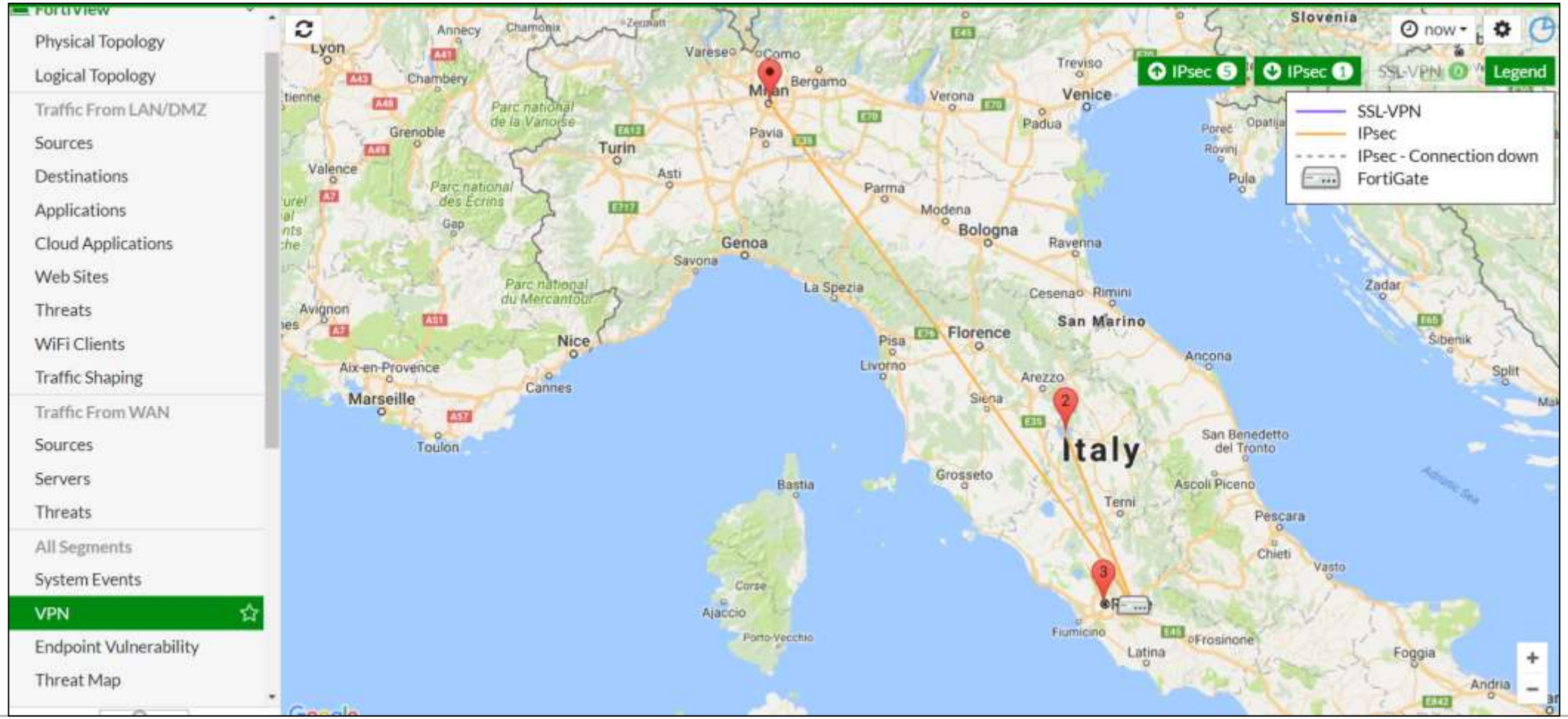
- Endpoints covered in the Security Fabric are ranked by their FortiClie
  - » Visible on 'E
  - » Score is calc
  - » Supports dri



Demo – FortiView

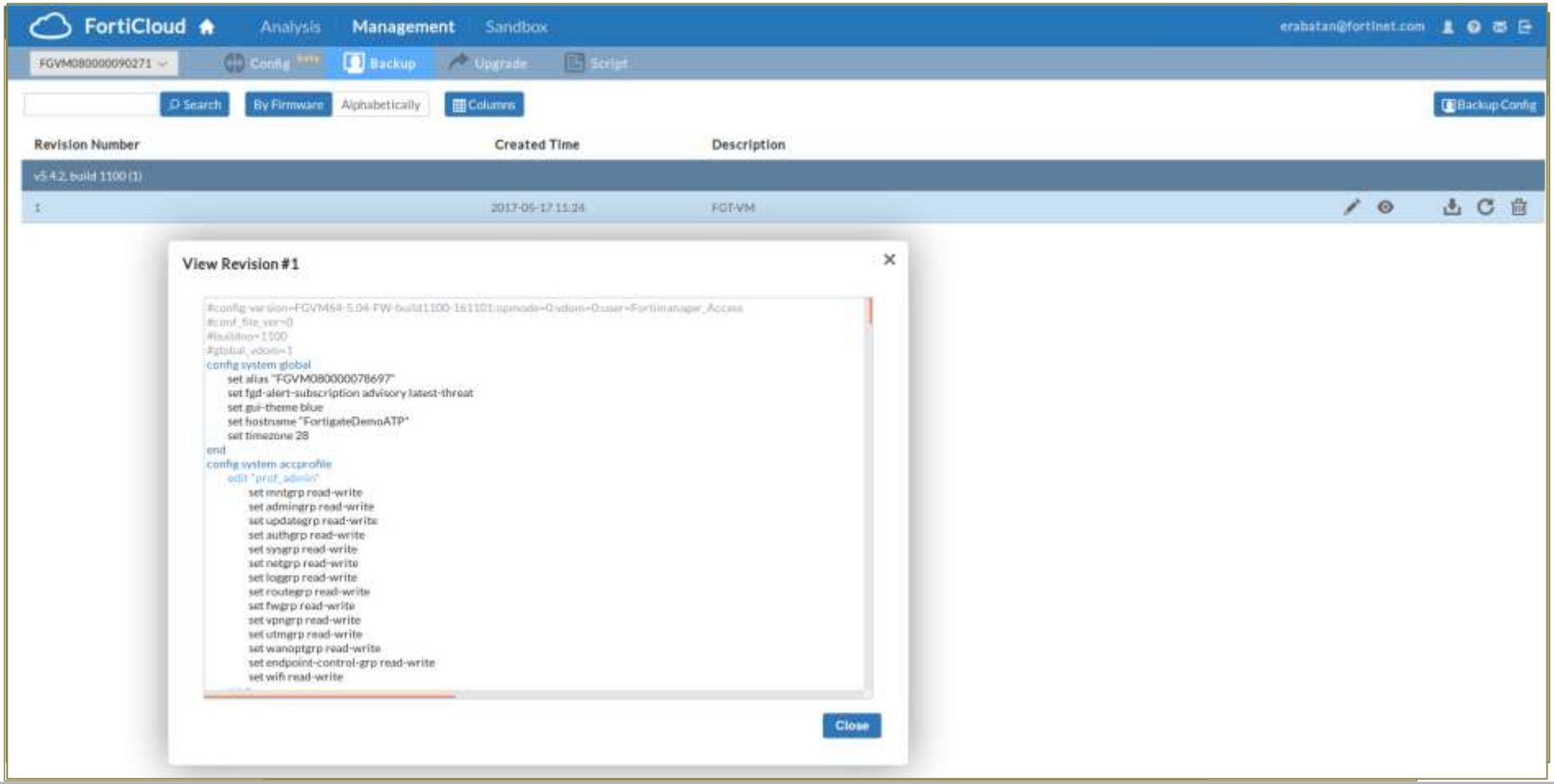
VPN tunnel map

- Help to materialize VPN tunnels on a map and quickly check their status



Central Visibility on Forticloud Fabric

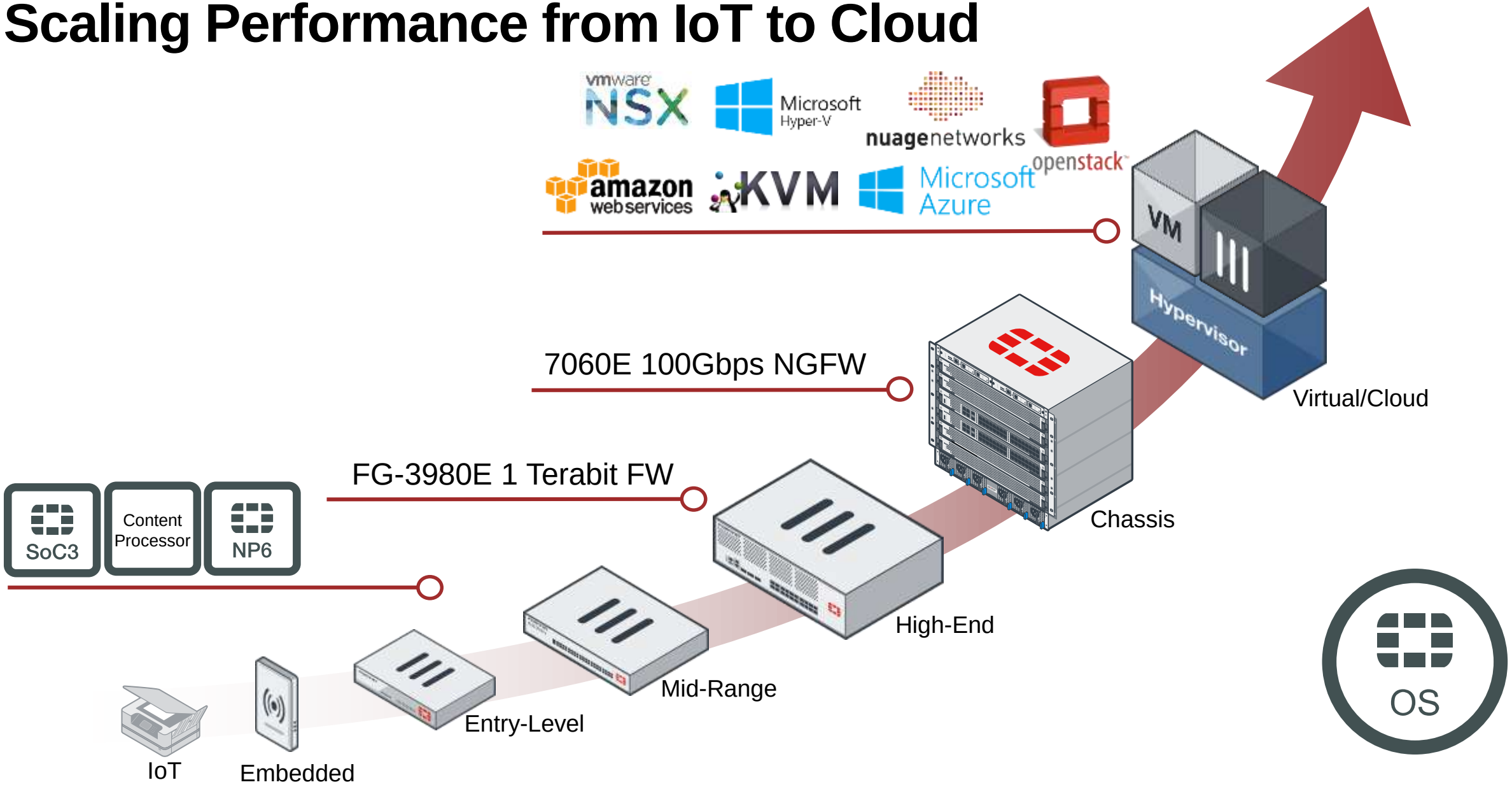
- All security components and virtual services available through one click



POWERFUL

Accelerated cloud-scale and security processor-based appliances with coordinated logging **to enable maximum threat protection without affecting performance**

Scaling Performance from IoT to Cloud



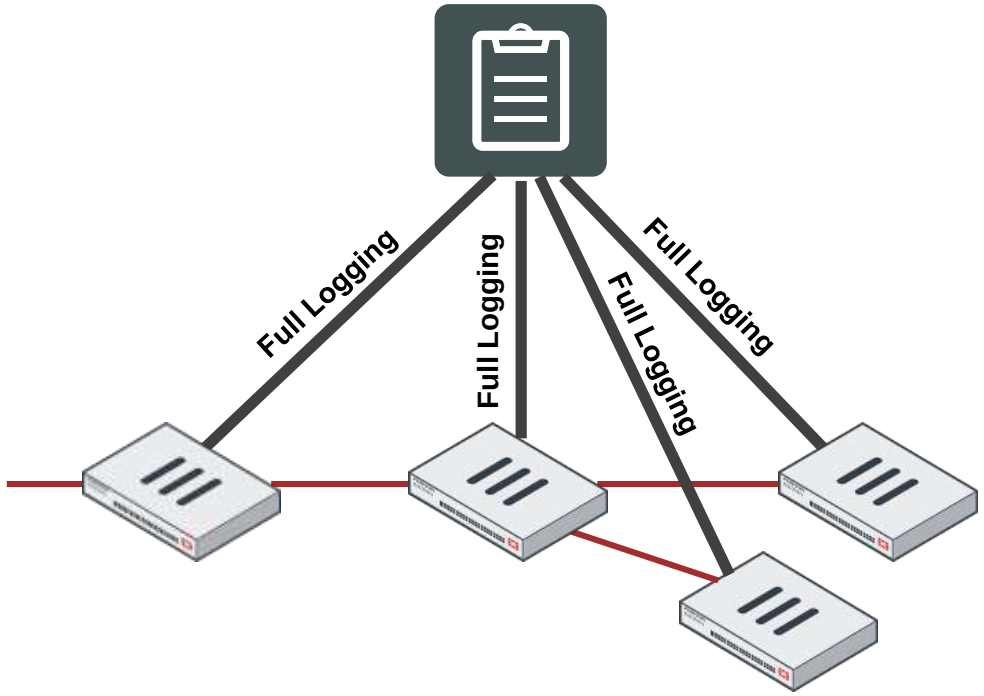
Hardware Acceleration

- NP6 Host protection engine
  - » Host protection against DDoS attacks at NP level
  - » CLI Option, apply to each NP6 processor separately
  - » User may set threshold based on each packet type (eg. TCP SYN) based on packet per second

- nTurbo (fastpath from external interfaces to IPS engine)
  - » Acceleration for sessions with flow-based security features
  - » Complete CP (pattern matching/pre-matching)

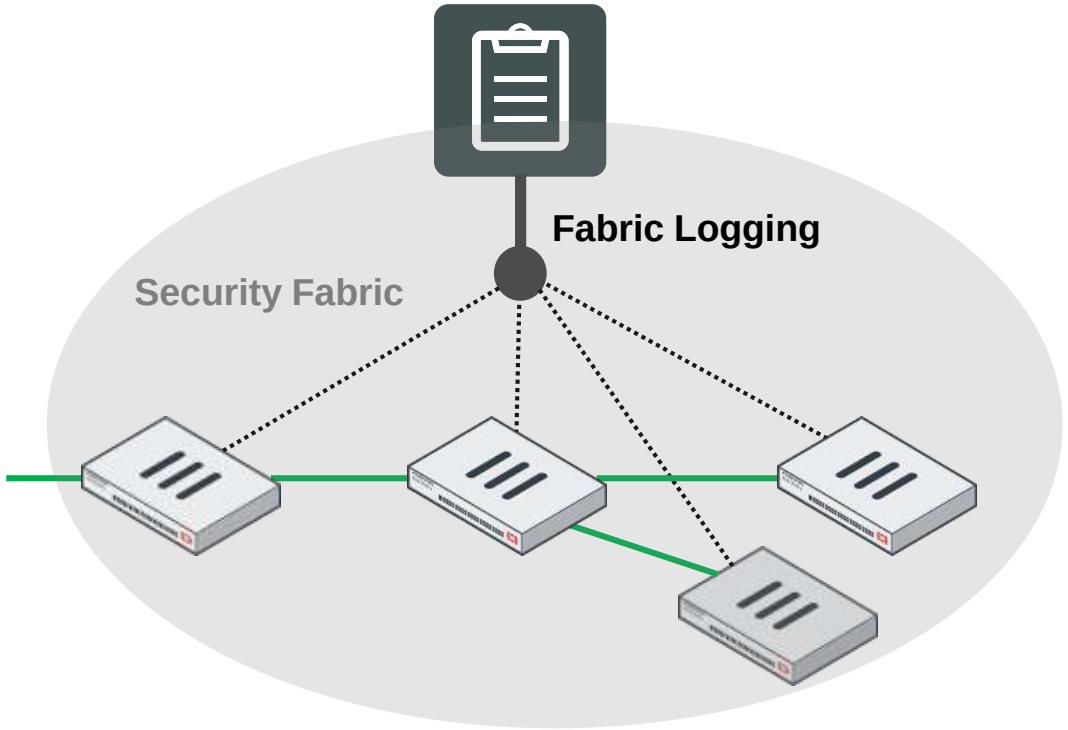
Coordinated Logging allows deep visibility and Better Performance

Uncoordinate



- Manual setting for each device for logging
- Each device sends full logging to FortiAnalyzer

Coordinated



- Automatic setting of all devices for logging
- Topology aware – log only what's needed

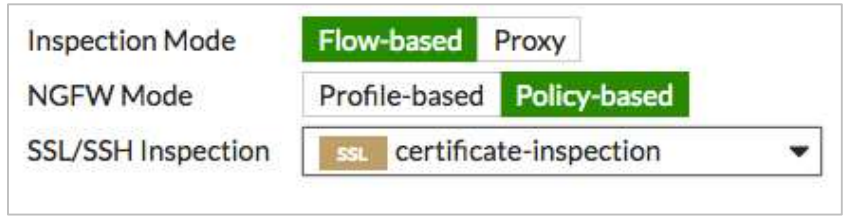
VM Enhancements

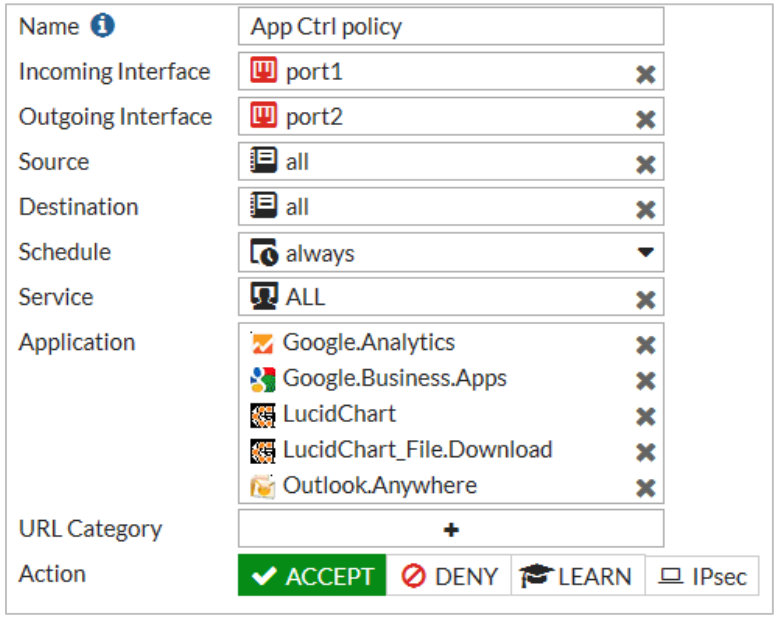
- Expand capacities and capabilities
  - » New VM with more vCPUs / memory up to 500 VDOMs
  - » VM08-UL support FortiOS Carrier Upgrade
  - » Number of virtual interfaces that FG-VM raises from 3 to 10

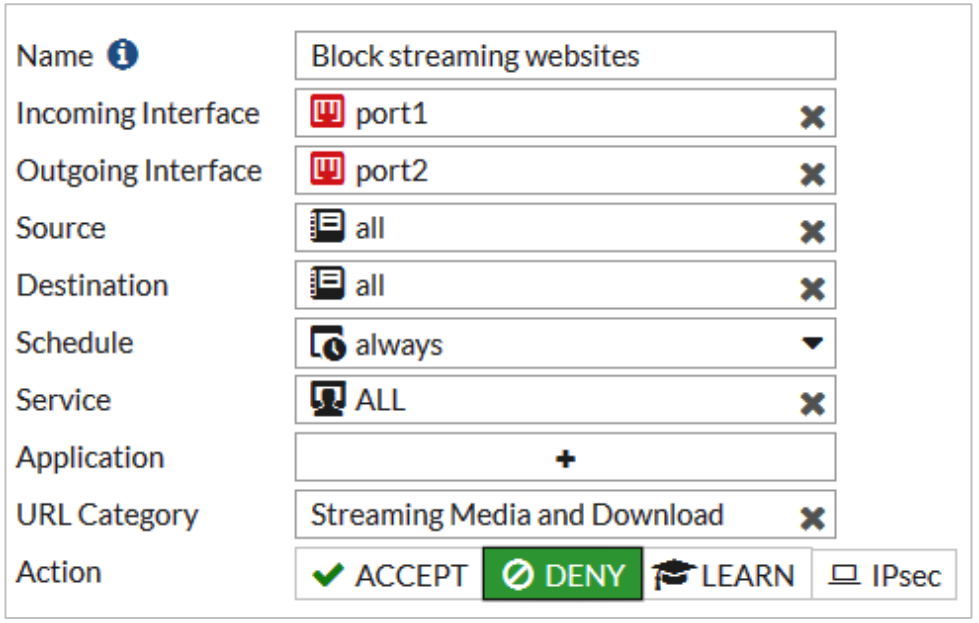
- Competitive pricing
  - » Cheaper VM option without VDOM capability for VM01 to VM04

NGFW Policy-based mode (1/2)

- Applications and/or URL categories can now be used as policy objects
  - » Requires flow-based mode and SSL insp.
  - » More flexible policy implementations
  - » Enables fall-through setups based on apps and web categories

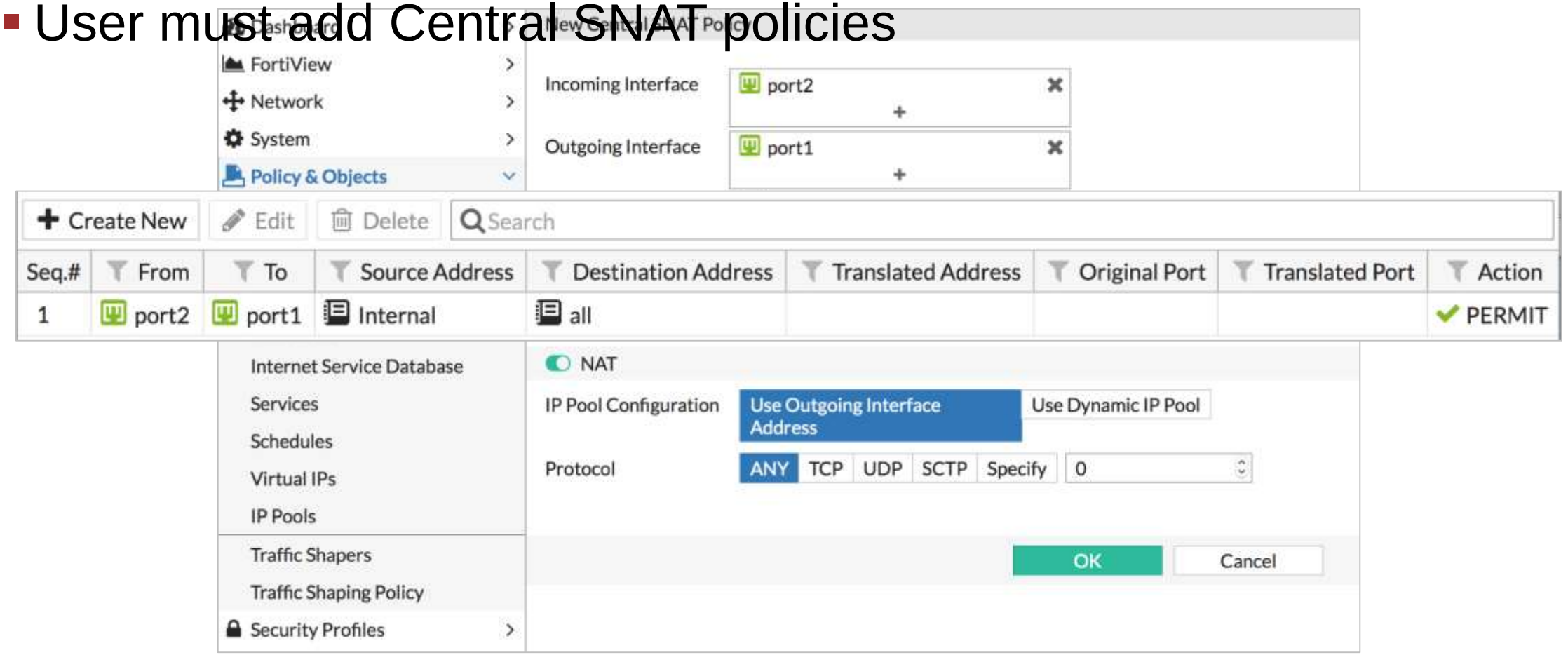






NGFW Policy-based mode (2/2)

- Enables Central SNAT for the policies
- User must add Central SNAT policies



Security Audit

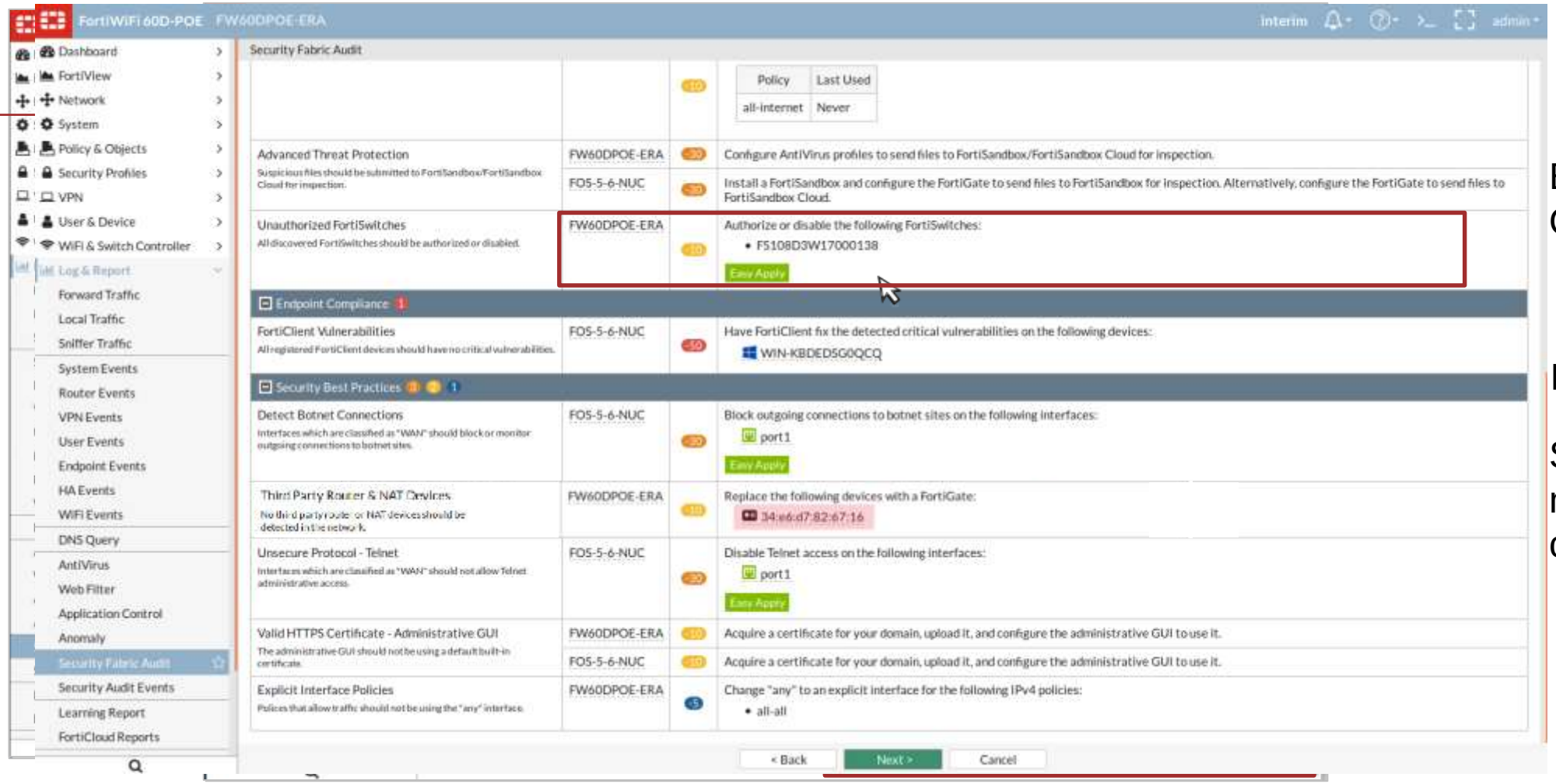
Security Fabric Audit

- Even the best tool can be misused
- Need assis
  - » Mistakes
  - » Best practi
  - » Consistenc
  - » …

Security Fabric Audit

- Automatizes a full security audit on the configuration of the Fabric

Score



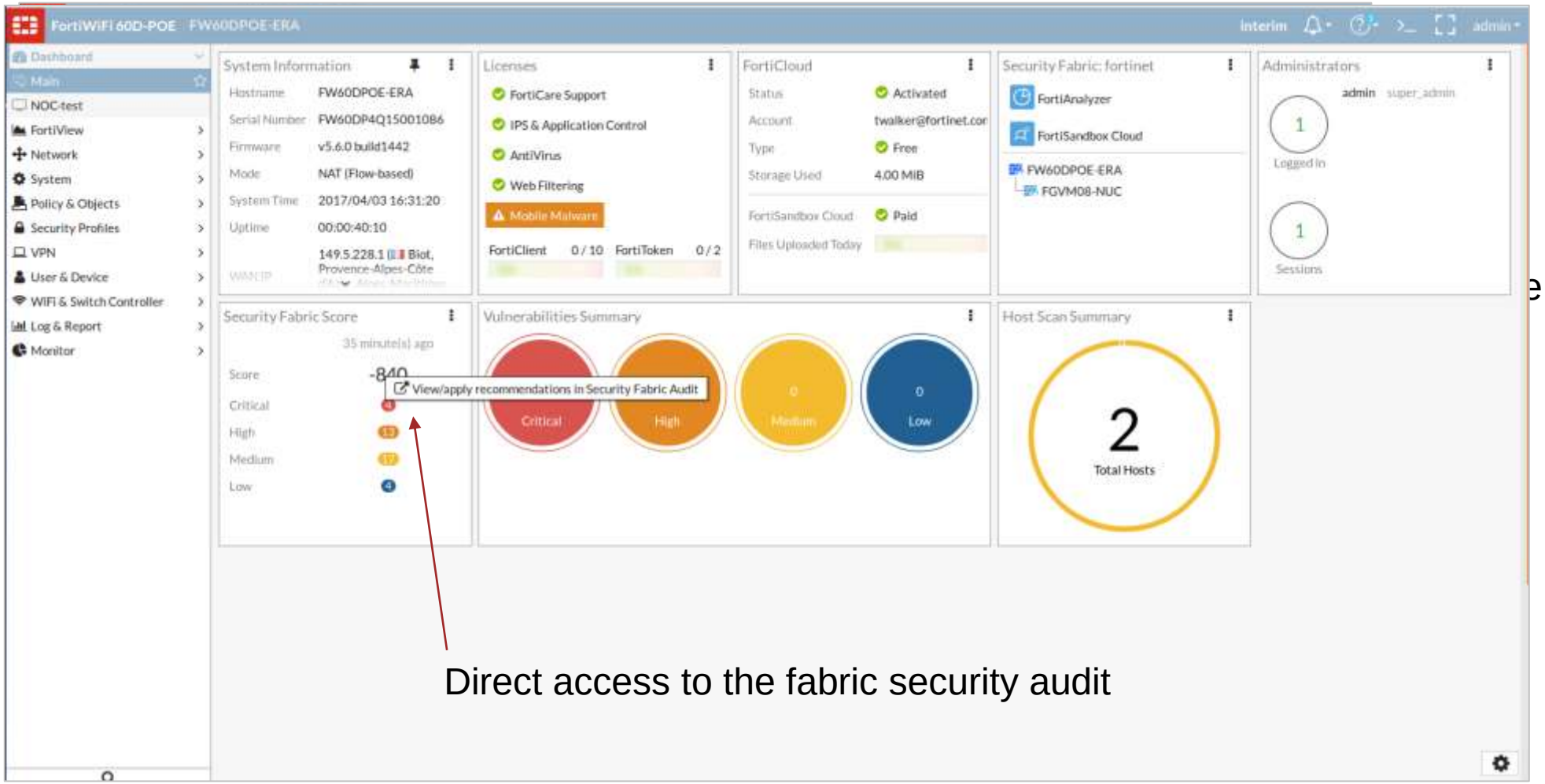
Easy Apply Only

Easy Apply

Select then make changes

New “Risk” widget from the Dashboard

- Risk widget provides the score for the security audit in a sec…



e resized

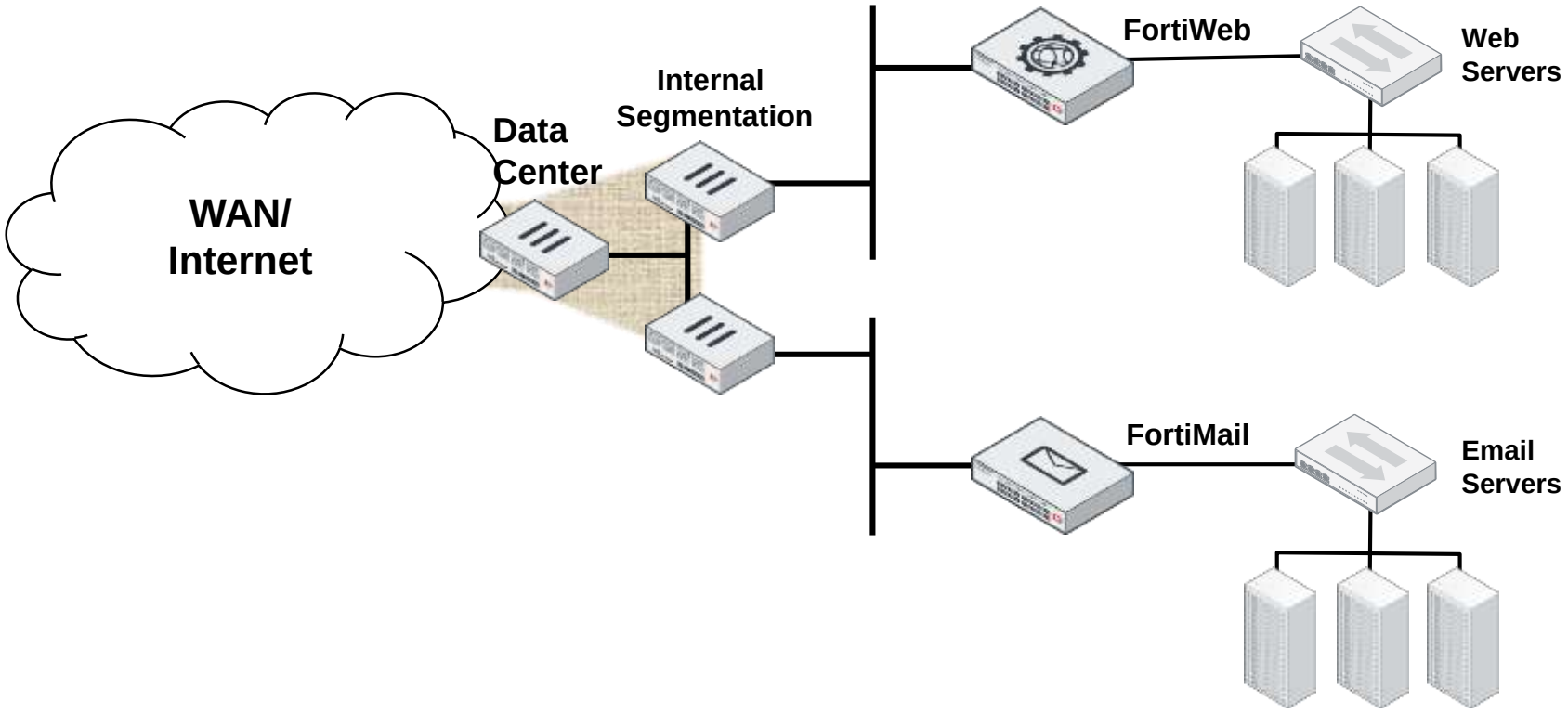
Direct access to the fabric security audit

Demo – Security Fabric Audit

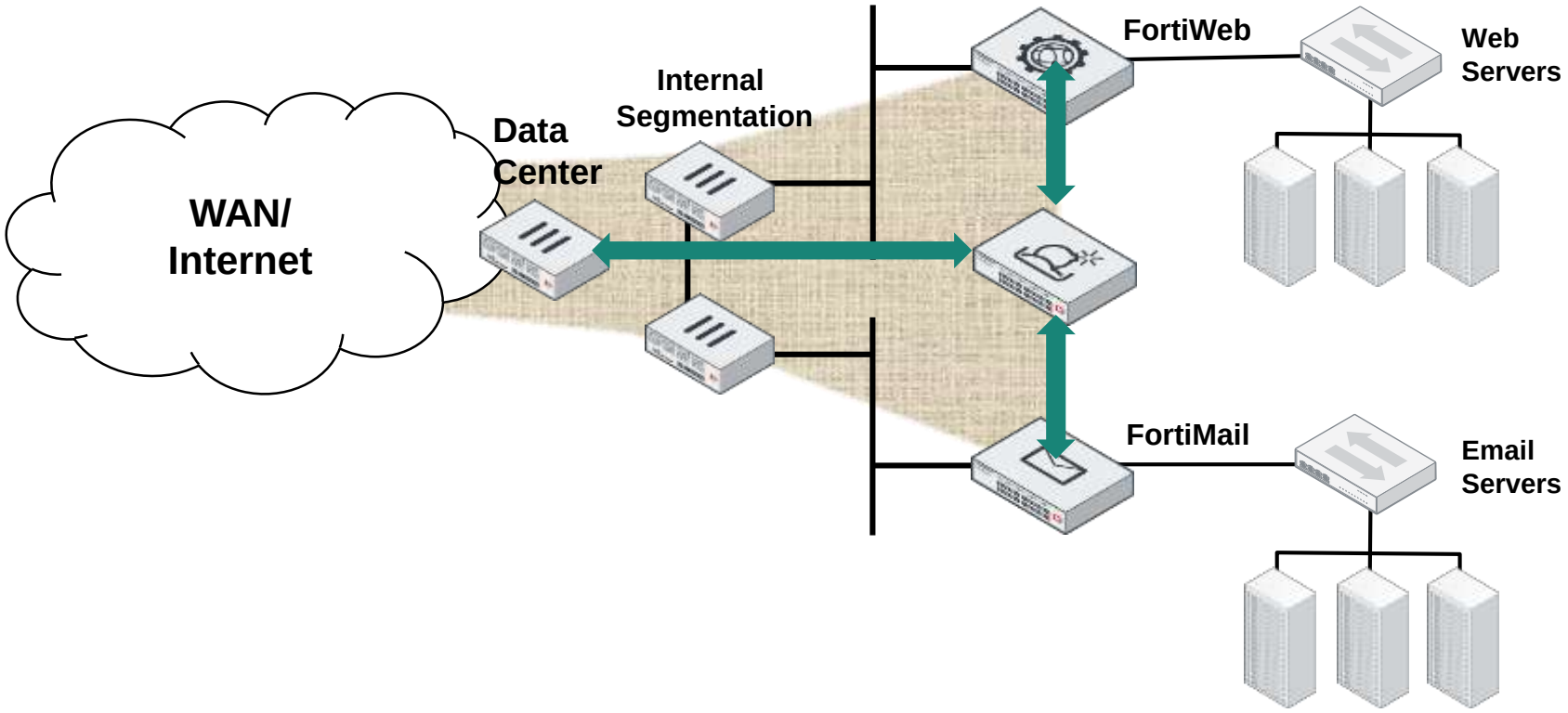
AUTOMATED

More efficient operations with new Security Fabric audit/recommendations, intelligence sharing, and NOC views

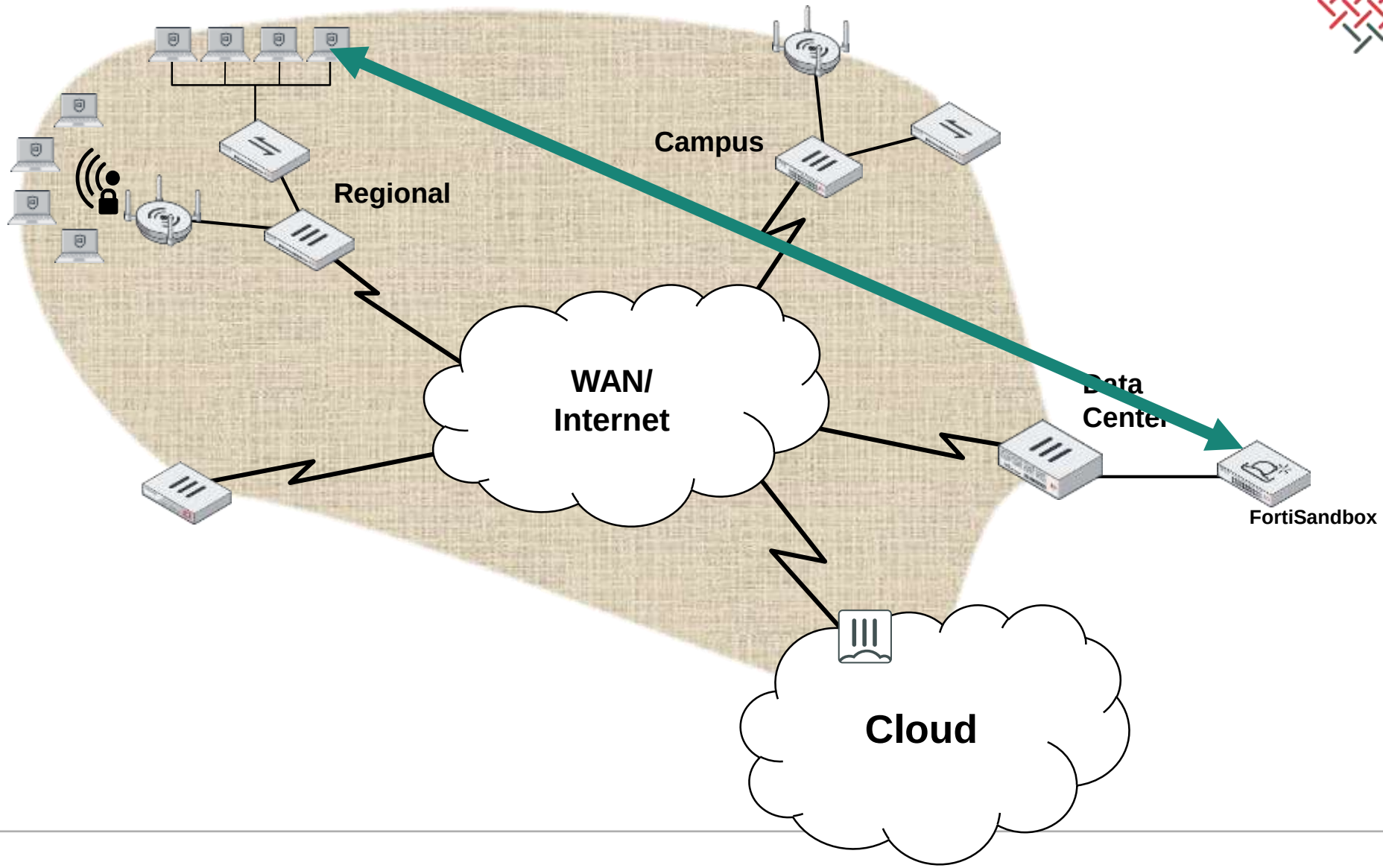
Meanwhile, Back in the Data Center…



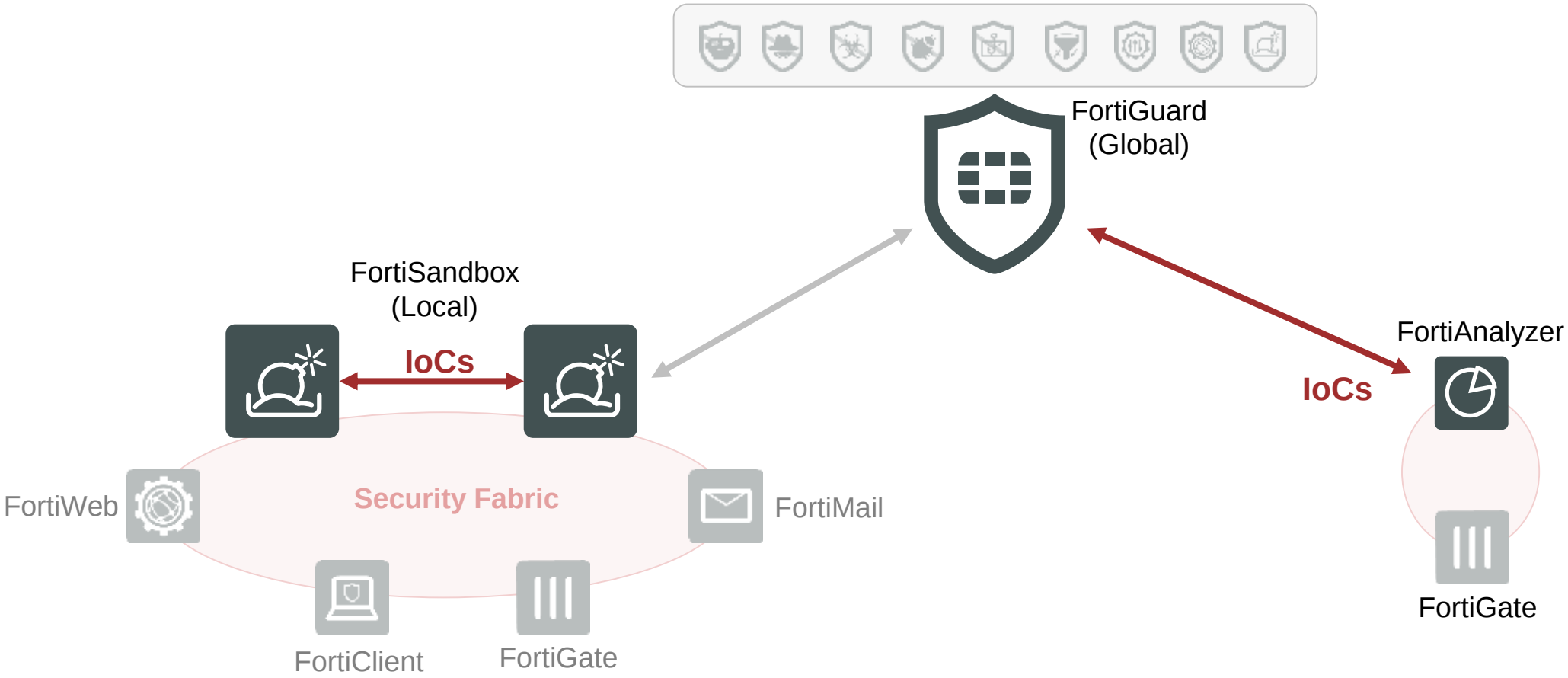
In the Data-Center



Extending Advanced Threat Protection to the Desktop



Rapid Sharing of Global and Local Threat Intelligence



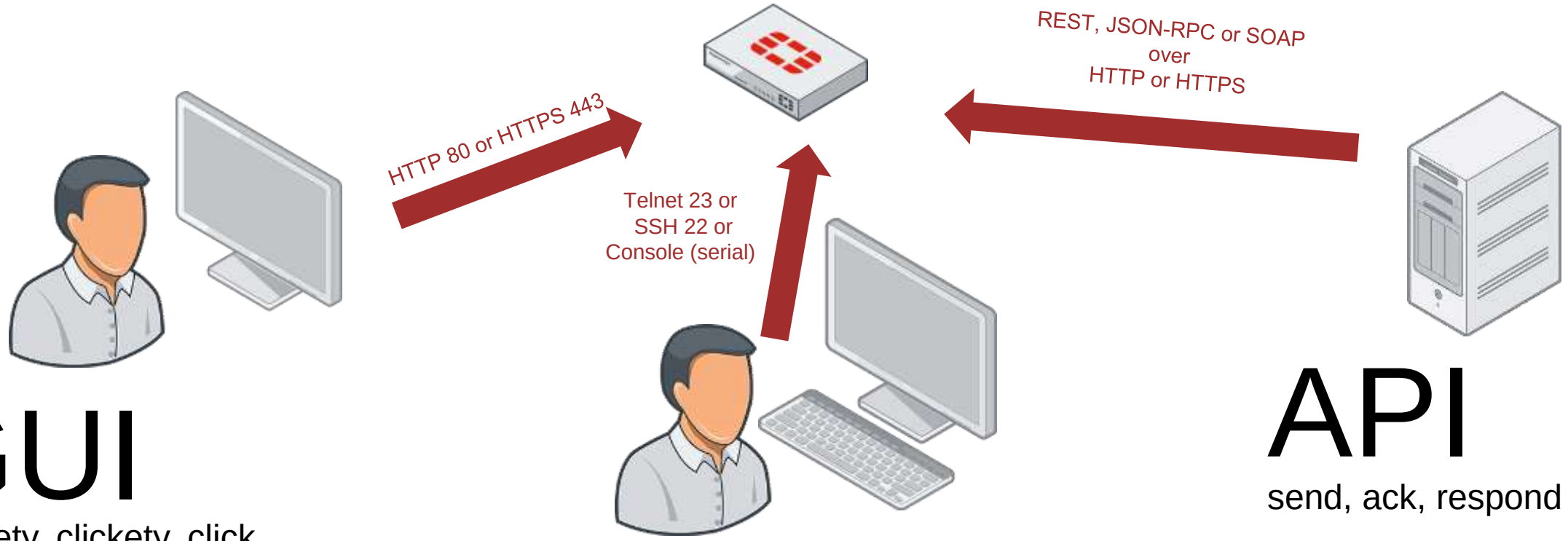
Clustered Local Intelligence distributed throughout the Security Fabric speeds mitigation

Correlation of Global IoCs and networking logs pinpoints new threats

Demo – Advanced Threat Prevention

What is an API?

API – Application Programming Interface “system talking to systems”



GUI

clickety, clickety, click

- Can’t config everything
- Slow
- Costly

CLI

typety, typety, type

- Slow
- Costly

API

send, ack, respond

- Hard to learn ?
- Might not do everything ?

Which products have an API?

FortiGate

FortiManager

FortiAnalyzer

FortiSandbox

FortiAuthenticator

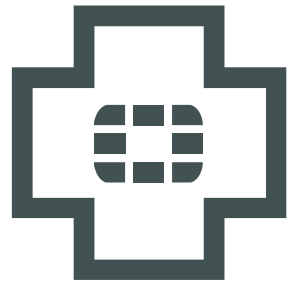
FortiWeb

FortiMail

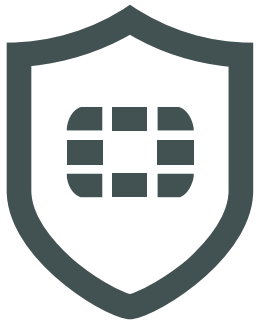
FortiDDoS

FortiCore

more

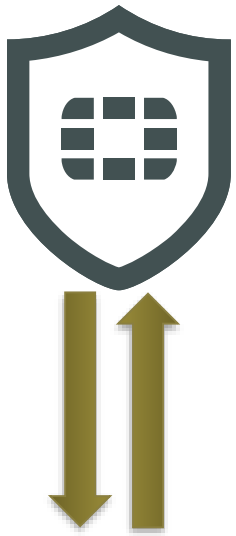


FortiCare



FortiGuard

API Use Case: FortiProvision with FortiDeploy



FortiGate CPE

Customer SIEM

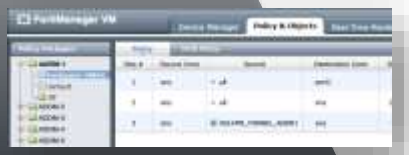
CEF logs

logs

FortiAnalyzer

- Provisioning complete
- Device registers
- Awaits instructions

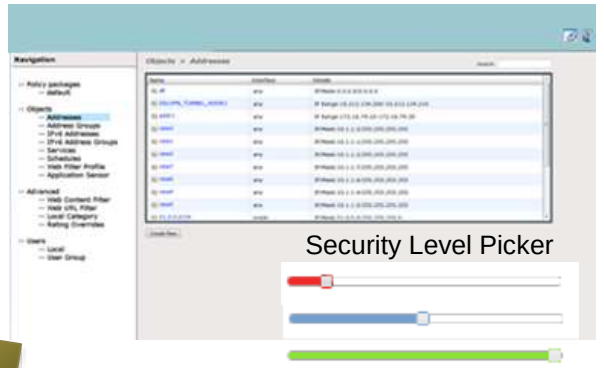
MSSP
FortiManager(s)



Device DB

Policy Packages

Customer Portal



REST/JSON

Customer choices in customer portal sent via API

- Provisioner applies template based on user/svc class

Provisioning Server

REST/JSON

SOAP/XML

- Turns on device
- Device auto-provisions over LTE
- Optional wired network later; LTE becomes backup

- Multi-tenant management
- Configuration repository / backups
- UTM/NGFW signature updates
- Firmware updates

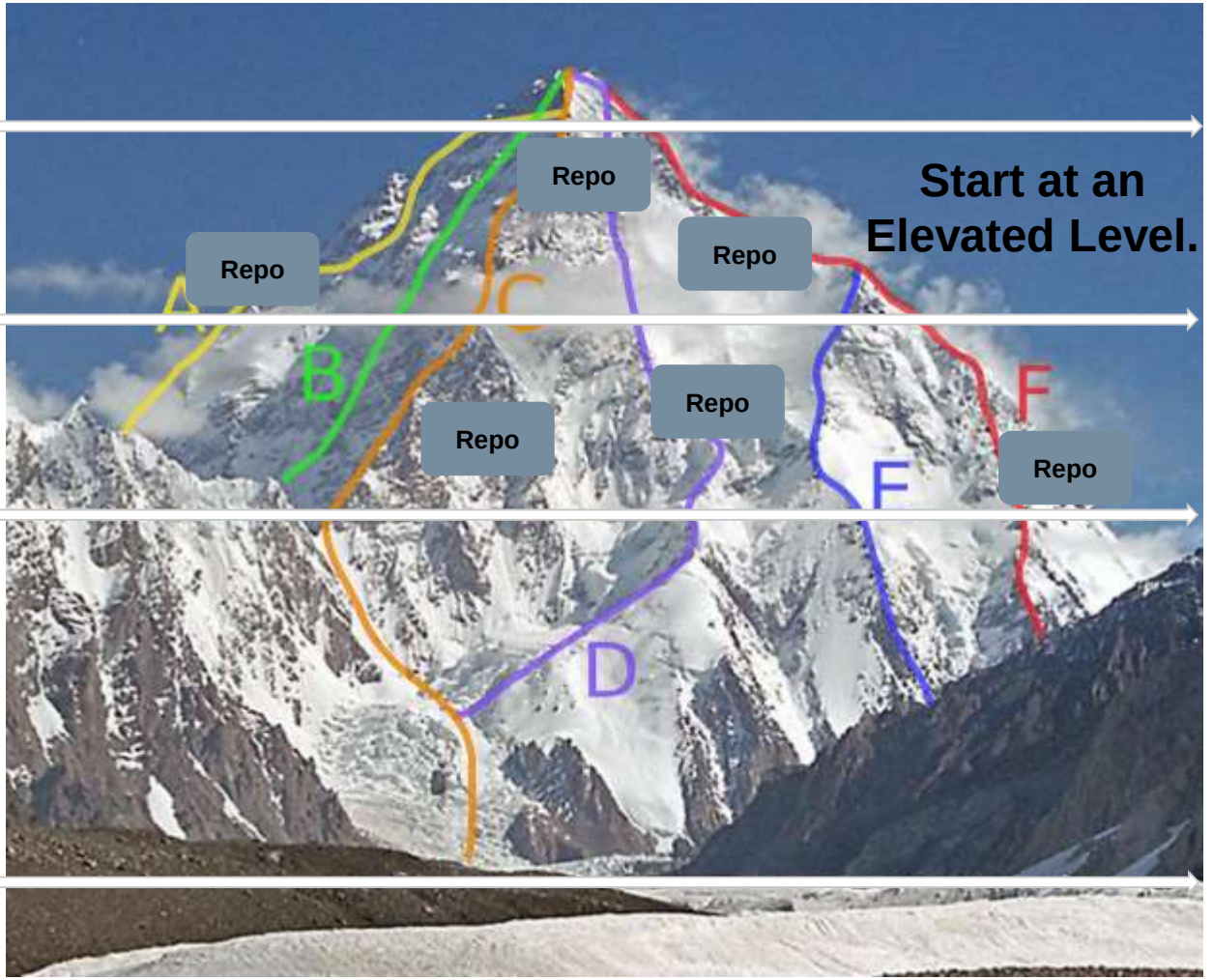
Automation Jump Start - FortiToolkit

MSSP Customized FortiToolkit

MSSP Partner FortiToolkit Packages

FortiToolkit Base (from FNDN)

Normal user



Security Fabric Beyond FortiWorld

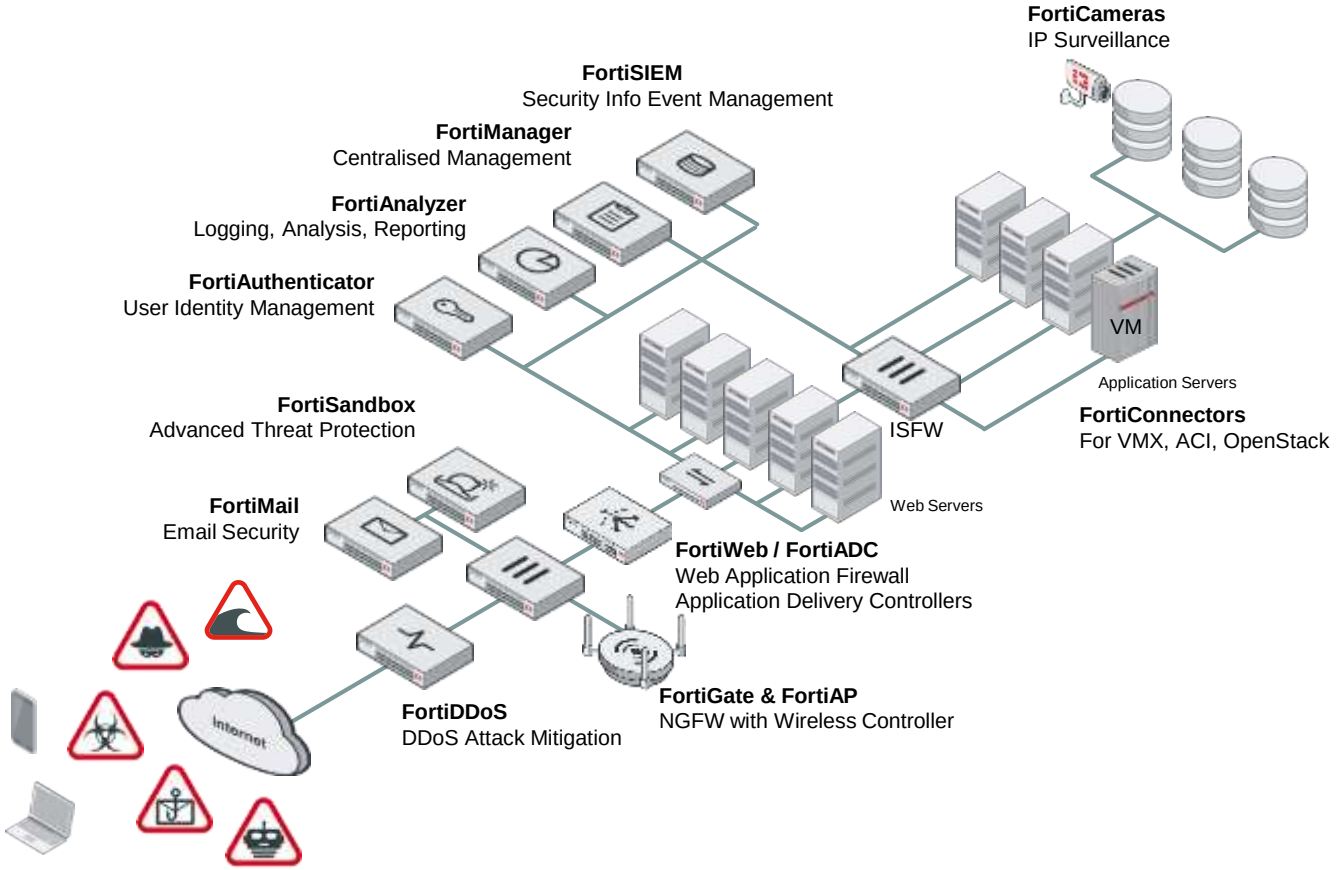
Fortinet Reference Architecture

Advance Threat Protection (ATP) Framework

FortiToken
Two Factor Authentication

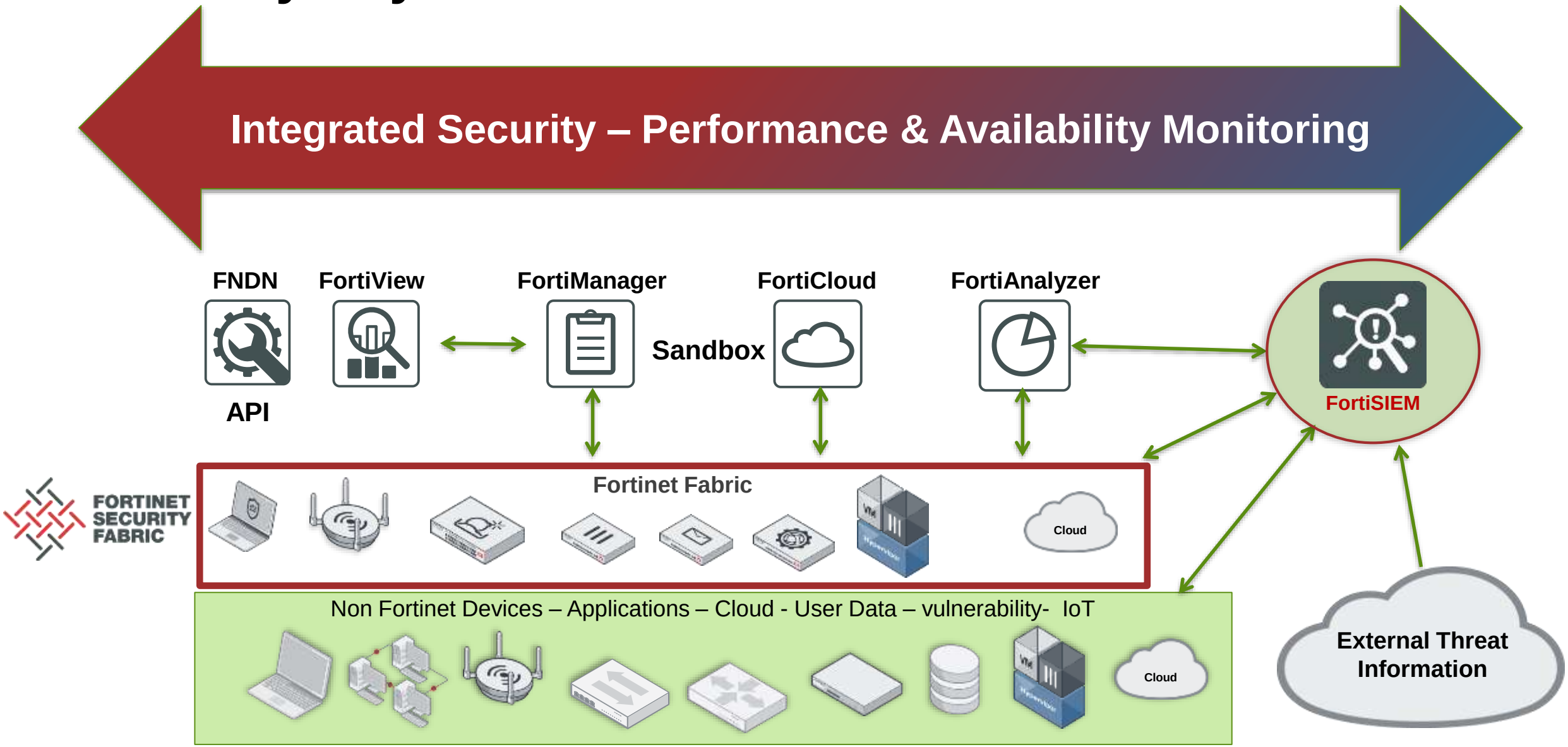
FortiClient
Endpoint Protection, VPN

AWS & Azure
Fortinet Solutions
FortiCloud Analytics & Management



Secure by FORTIGUARD™

Visibility Beyond Fortinet Products – FortiSIEM!



Broad – The Fabric Gives You Complete Visibility, Coverage and Flexibility Across The Entire Dynamic Attack Surface

FORTINET SECURITY FABRIC

Visibility

Coverage

- Cloud Security
- Application Security
- Network Security
- Access Security
- Client/IoT Security

Flexible/Open

Technology Alliance Partners leverage Fabric APIs, Logging, Auth & Threat Intelligence for integration

Fortinet Fabric-Ready Partner Program

- Leverages Security Fabric APIs to deliver pre-integrated, end-to-end security offerings
- Integrated products improve threat awareness & intelligence, broaden & coordinate threat response and policy enforcement
- Faster time-to-deployment & reduced costs due to pre-validation of solutions
- Fabric-Ready Program is a Premium category of Fortinet's Technology Alliance Partnerships
- Alliance Partnerships web page: https://www.fortinet.com/partners/partnerships/alliance-partners.html

Fortinet Security Fabric

Fabric-Ready Partner Program
Benefits for Channel Partners

- Deliver more effective, more responsive security solutions that leverage the collaborative power of the Fortinet Security Fabric
- Speed business outcomes with integrated ecosystem solutions that address customers' needs. Through Fabric-Ready pre-validation, gain access to more opportunities you can quickly sell into
- Leverage Fortinet's Fabric-Ready seal of approval to build trust with customers and instill confidence that the solutions work
- Deliver solutions with faster time-to-deployment to customers, with reduced technical support burden & costs due to pre-validation

Fortinet Technology Alliance Partnerships

OPEN

Virtualization & SDN/NFV

Fabric Ready: Brocade, Cisco, nuagenetworks, Ubiqube, Silver Peak, Versa Networks, VMware NSX, Pluribus Networks, Arista, big switch networks, Citrix, Corsa, NEC, Ericsson

CLOUD

Fabric Ready: VeriSign, Oracle, HPE Helion, velocloud, amazon web services, Microsoft Azure, NTT, HyTrust, IBM Cloud, Sonus

ENDPOINT & IoT

Fabric Ready: Carbon Black, Nozomi Networks, SentinelOne, ForeScout, Attivo Networks, Pulse Secure, ziften

MANAGEMENT

Fabric Ready: Qualys, tufin, WhiteHat Security, Centrify, algosec, Gigamon, Bradford Networks, Eleven Paths, gemalto, Kiana Analytics, FIREMON, skybox Security, Extreme

SIEM

Fabric Ready: Hewlett Packard Enterprise, IBM Security, splunk>

SYSTEMS INTEGRATOR

Fabric Ready: Hewlett Packard Enterprise, IBM Security, Capgemini, dimension data, NTT Communications, accenture

Fabric-Ready Partners

Cisco

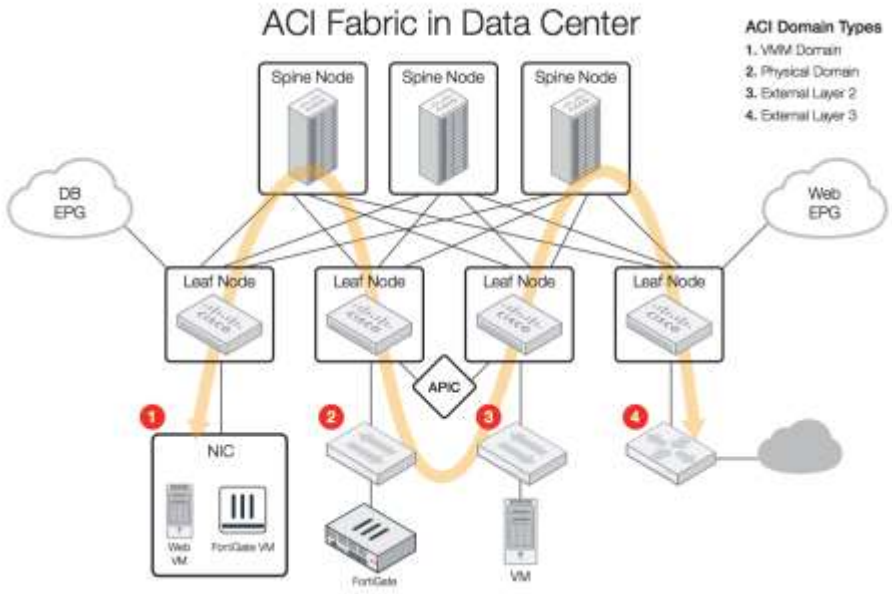
Key Solution Features

- The integration of Cisco ACI architecture with FortiGate provides automated, predefined policy-based security provisioning and security policy updates for NGFW, UTM and VPN services.
- Single-pane-of-glass management enablement from Cisco APIC with full visibility on security policy enforcement.
- Predefined security policies are deployed rapidly through complete application deployment lifecycle
- Consistency and transparency across physical and virtual application workloads, and scale on-demand with automation.

Key Benefits

- Better visibility and security correlated with overlay/underlay networks.
- Lower TCO from reduced administrative OPEX Accelerated application and L4-L7 security deployment.
- Increased efficiency in service provisioning and network security segmentation.

Integration: Virtualization & Management APIs



Fortinet-Cisco ACI Solution

Solution brief:
https://www.fortinet.com/content/dam/fortinet/assets/alliances/Cisco-ACI-SolutionBrief.pdf

Fabric-Ready Partners

Nozomi Networks

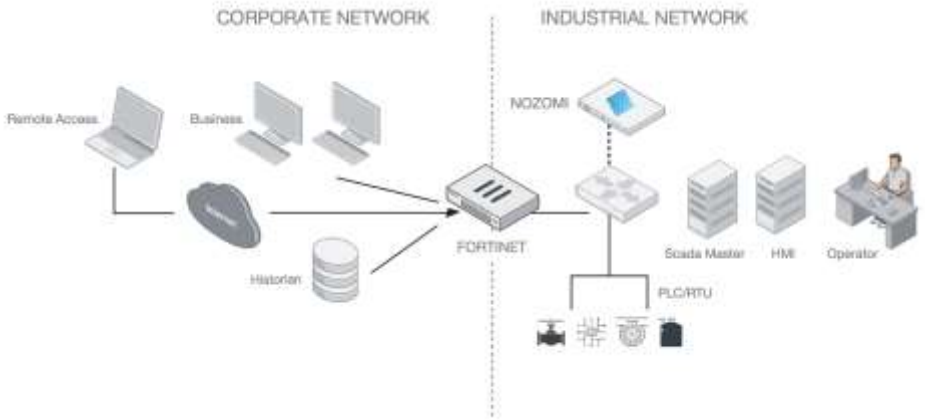
Key Solution Features

- Nozomi SCADAguardian implements innovative technology for monitoring and assessing Industrial Control Systems.
- Connects to the industrial network non-intrusively and in a fully passive mode, listening to all traffic between the control and field networks, analyzing it at all levels of the OSI stack (from L1 to L7).
- Uses Artificial Intelligence and Machine Learning techniques to create detailed behavior profiles for every device according to the process state, detecting critical states in the process.

Key Benefits

- Enhance security for ICS networks via sophisticated detection of ICS security issues with proactive threat remediation and containment.
- Reduce operational complexity and costs via centralized management, logging and reporting.
- Provides best-in-class visibility, security, monitoring, alerting, reporting, troubleshooting, and forensic capabilities.

Integration: Endpoint and Management APIs.



Fortinet-Nozomi Networks Solution for Securing Industrial Control Systems

Solution brief:
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Fortinet-Nozomi.pdf

Fabric-Ready Partners

Qualys

Key Solution Features

- Qualys Web Application Scanning (WAS) is a cloud service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection.
- The integrated solution that scans applications for vulnerabilities with Qualys WAS and protects them with Virtual Patching on the FortiWeb WAF. Once a vulnerability is discovered, it's protected by FortiWeb instead of issuing disruptive emergency patches.

Key Benefits

- Fewer disruptions due to emergency fixes and test cycles by virtually patching vulnerabilities until they can be permanently fixed.
- Reduced risk of exposure to threats between the time a threat is discovered until it is fixed by developers.
- Protection for legacy, inherited, and third-party applications where development fixes aren't an option or are impractical.

Integration: Management APIs.

Fortinet-Qualys Solution for Web Application Vulnerability Scanning and Virtual Patching

Solution brief:
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Fortinet-Qualys.pdf

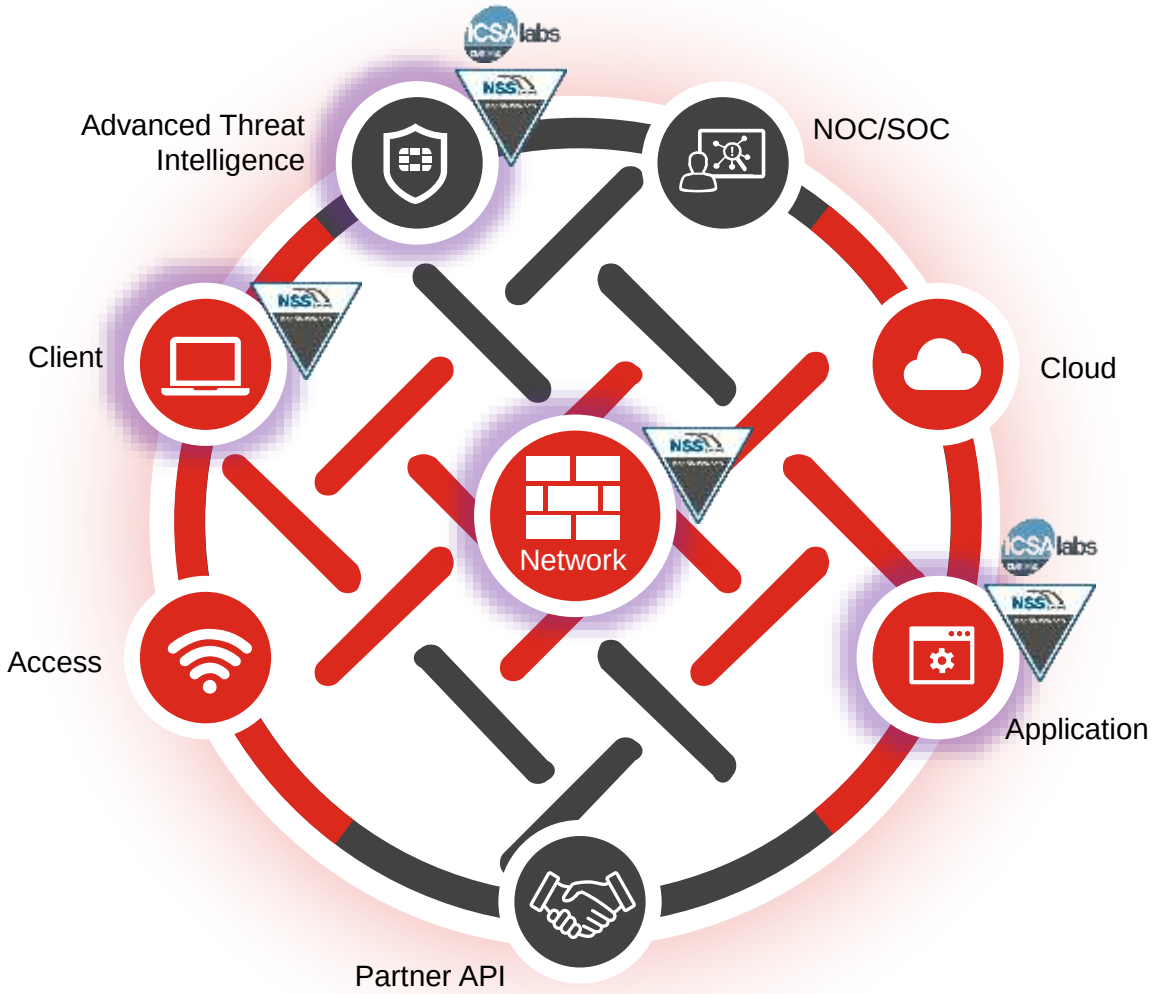
Summary

Let’s keep some pieces!

What we have Covered in this Training

- Security Fabric Vision
  - Tight mesh of interconnected security controls
- Broad solution
  - Be informed about your environment, regardless what it looks like
  - Demo FortiView
- Powerful solution
  - Don’t let security be an inhibitor, but an enabler
  - Security Fabric Audit demo
- Automated solution – profit to the max
  - Coordinated Advanced Threat Protection – demo
  - Go beyond FortiWorld

Only Vendor NSS Recommended At All Layers: Network, Application and Endpoint



FORTINET SECURITY FABRIC

- **Broad**
- **Powerful**
- **Automated**


FORTINET